Technical Report

SADRA:
A Sound Capability-based Access-Control
System for Disaggregated-Resource
Architectures

Contents

List of Tables

1 Introduction

Resource disaggregation strives to optimize resource utilization and improve elasticity by decoupling existing resources, such as CPUs, memories, and accelerators, from *processing elements* (PE) and distributing them into pools of heterogeneous resources, which PEs can access via fast mediums [34, 5, 13, 38, 47, 56]. Driven by the growing resource demands, disaggregated-resource architectures have recently attracted considerable attention from academia and industry [42, 22, 4, 3, 23, 25, 37, 9, 24, 2, 15]. For example, various architectures and applications, such as *data centers* [33, 54, 43], *blade servers* [41], *rack-scale systems* [61, 51, 55], *cloud frameworks* [39, 8, 11], and *high-performance computing* [64, 36], have employed resource disaggregation to enhance their efficiency and performance.

Despite optimizing resource utilization, the distributed nature of disaggregated resources raises concerns about controlling access to them, such as: how an architecture provides fine-grained resource allocation for distributed resources; how it prevents processes from accessing unauthorized resources; and, how processes can delegate their access rights or revoke shared privileges. Furthermore, some disaggregated-resource architectures leverage *one-sided* communication—they replace processor/-software stacks on resource sides with hardware-based controllers— to improve performance [20, 48, 9, 34]. These controllers receive requests and directly read/write from/to resources based on them, thus raising security and privacy concerns [63].

Supporting elasticity introduces a new challenge to access-control systems. Elasticity in disaggregated-resource architectures means the ability and flexibility to scale [27, 31, 65]—resources and PEs should be able to attach to an architecture with minimum adaptation. For example, consider *Memory-Driven Computing* (MDC) [35], an abstract disaggregated-memory architecture comprising a pool of byte-addressable *Non-Volatile Memory* (NVM) modules and a fast-speed fabric. The architecture enables diverse PEs, such as CPUs and FPGAs, to attach the fabric and use the shared memory for storing data and other purposes, such as communicating channels. Nevertheless, an adversary process can access other processes' data by knowing data references. Thus, any suitable access-control system should support newly attached resources and PEs but cannot rely on PEs to control access. MDC demonstrates why a scalable and fine-grained access-control system is critical for these architectures; it provides direct and indirect access to a distributed and byte-addressable persistent shared memory for different PE types.

Recent works show that the *capability-based access-control* model [18, 21, 12] best suits disaggregated-resource architectures [10, 28]. The capability-based model employs unforgeable tokens, namely *capabilities*; thus, it can address various resource types, such as memory or computing resources. Furthermore, it provides a scalable and fine-grained controlling mechanism [10]. Moreover, it supports the *least-privilege principle* [59], thereby allowing fine-grained delegating or revoking access privileges.

In this paper, we first conduct a comparative analysis of capability systems because researchers have proposed several capability systems for different architectures [52, 32, 30, 19, 14, 66, 12, 67, 58, 50, 57, 26, 1, 60, 40, 7, 6, 28]. We systematically reviewed existing capability systems to investigate which suit the architectures best.

While reviewing capability systems, we extracted six traits from them, including distributed structure, subject and object granularity, capability delegation and revocation, and persistency. These traits enable us to reason about the capability systems' efficacy, performance, and applicability regarding disaggregated-resource architectures. For example, non-distributed capability systems, such as *CHERI* [66], do not suit these architectures because the distributed trait is a fundamental demand. Furthermore, we checked if they require HW/SW support.

Our investigation demonstrates that none of the existing capability systems covers all the extracted traits, and implementing their designs may be unpragmatic. For example, consider *CEP* [6] and *SemperOS* [28], two capability systems that supports most traits. CEP only involves resource-side controllers, thus introducing performance overheads due to communicating with PE-side processes. SemeprOS expects PE manufacturers to implement and integrate its suggested method into their products, which renders its approach impractical. Because access control constructs the basis for any secure or privacy-preserving framework and none of the systems supports all the traits, we decided to design a suitable access-control system for disaggregated-resource architectures.

In the second part of this paper, we present SADRA, a general-purpose capability-based access-control system for disaggregated-resource architectures that supports all the above traits. Making a general-purpose system enables architectures to adapt and employ it according to their requirements. For example, they can adapt our system to support direct or indirect memory access. Furthermore, the distributed nature of our access-control system enables other architectures, such as *Grid computing* [16] and *GPU clustering* [45], to employ it to control access to their shared distributed resources. SADRA provides efficacy, performance, and applicability by controlling access as close to processes as possible and providing fast capability-hierarchies revocation. Moreover, it resolves the one-sided communication challenge using co-processors, eliminating the need for processor/software stacks.

Our system's design controls access at two stages using controllers at PE-sides and resource-sides (Section 4). PE-side controllers enable the system to start controlling access close to processes, reducing the workloads of resource-side controllers. In addition, PE-side controllers can handle internal delegation requests without involving other controllers. Resource-side controllers perform final controls before granting access to resources. Furthermore, they manage inter-PE delegations, which enables them to revoke capability hierarchies efficiently; thus, PE-side controllers never communicate with each other. Consequently, the above three characteristics make our access-control system a scalable one.

We verify that our capability-based access-control system is sound; every resource access must be via a legitimate capability containing appropriate permissions (Section 5). To formally verify the soundness, we prove our access-control system provides *capability safety* and *authority safety* properties using the *assumption-commitment* (A-C) method (Section 2.2). The capability-safety property guarantees that a process can only employ legitimately acquired capabilities that are still valid. The authority-safety property ensures that the upper bound of a process's authority is the authority of its valid capabilities, and no authority amplification occurs while delegating a capability. In addition, we prove that our design can guarantee *isolation* property based on

capability-safety and authority-safety properties. The isolation property states that accessible resources by processes are mutually exclusive.

We instantiate our access-control system for MDC as the use case (**??**). Memory disaggregation in MDC makes it a suitable case for demonstrating our access-control system; a resource is a byte-addressable memory range; the access-control system must provide direct and fine-grained access to memory while hiding the physical address of objects. We describe the instantiated system, illustrate its controllers, and verify that it is sound.

Finally, we model our design and check its correctness using the *SPIN* model checker [29].Specifically, we employ SPIN to check the safety properties based on the assumption-commitment method.

The contributions of our work are as follows.

- We present a general-purpose capability-based access-control system for disaggregated-resource architectures that covers the above qualitative criteria. Our system's design enables PEs to connect to architectures in a plug-and-play manner.
- We formally prove the soundness of our access-control design by verifying that it provides capability safety, authority safety, and isolation properties.
- We instantiate our access-control system for MDC.
- We model our access-control system and check its correctness using the *SPIN* model checker.

2 Background

This section describes the capability-object model, explain the A-C method, describe MDC, and state our threat model.

2.1 Capability-Object Model

Capability-based access-control model provides flexible techniques to enforce the least-privilege principle by sharing authority via unforgeable tokens, namely *capabilities* [18, 21]. Miller et al. [46] introduced the *capability-object model* as a security measure to control access to particular system parts, in which *object*s represent system resources and subjects. Furthermore, the model employs capabilities to encode access rights and enable objects to interact via them. A *capability* is an unforgeable token that refers to a specific object in this model.

When an object possesses a capability, it can communicate with the referred object. For example, imagine three objects: A, B, and C. Object A owns a capability referring to C and wants to delegate the capability to B. To accomplish this, A first creates two mediator objects, R and F, as depicted in Figure 1. Object A only provides B with access to F and asks objects R and F to forward B's requests; thus, B can access C through them. To revoke the access, A asks R to stop delivering B's messages, which renders B'access to F useless. Miller refers to objects R and F as *revoking facet* and *forwarding facet*, respectively. We follow Miller's approach to design our access-control system (Section 4.3).

2.2 Assumption-Commitment Method

The assumption-commitment (A-C) method [49, 17] is a compositional technique for specifying and verifying the interaction between a process and its environment, which makes it a suitable tool for reasoning about *concurrent*, *open*, and *reactive systems*. It facilitates reasoning about a system by isolating its processes and reasoning about them, where an isolated process communicates with its environment via synchronous message passing.

For reasoning about a process (p), the method requires information about four quantities: (1) The process's initial state; (2) The process inputs' properties; (3) The properties that each process's output fulfills; and (4) The process's final state. Precondition ϕ, assumption A, commitment C, and postcondition ψ provide the information for the method. Assumption A expresses what the process can assume about its prior inputs from its environment during its execution. Commitment C indicates what the environment can expect about the process's outputs. The method specifies the process with the following A-C correctness formula:

$$\langle A,\, C\rangle :\ \{\varphi\}\ p\ \{\psi\}$$

The process satisfies the A-C specification if it guarantees commitment C as long as the environment respects assumption A.

The method examines if assumption A and commitment C hold after each message exchange. It uses state machines to present and reason about the sequential segments

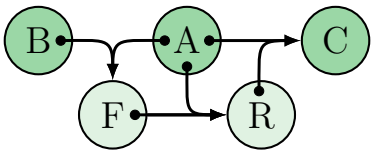


Figure 1: Capability-Object Model.
Legend: F: Forwarding Facet; R: Revoking Facet

of a system. Tuple (L, T, s, t) expresses the sequential transitional diagram of a component, in which L presents a final set of locations, T defines a final set of transitions, s is the entry point, and t is the exit location. The method refers to the above tuple as a *program*.

The A-C method leverages an *assertion network*, Q, to define the state of locations in a component's diagram. The assertion network assigns a predicate, Q_l, to each location, $l \in L$, in the diagram, which expresses the location's internal state and communication history. Furthermore, the method uses a *logical variable* to track the history of the component's communications.

The assertion network and the logical variable enable the method to reason about the component using the *assumption-commitment-inductive assertion network*, $Q(A,\ C)$, concept. To show that an assertion network is A-C-inductive, the A-C method checks if the predicate Q_l and assumption A imply predicate $Q_{l'}$ during the transition from location l to l'. Furthermore, if outgoing communication occurs during the transition, the method checks if the transition satisfies commitment C.

The method uses *Parallel Composition* rule to reason about parallel-executing processes w.r.t. their assumptions and commitments.

Rule 1. *The* A-C *correctness formula of two parallel executing processes,* $p \stackrel{def}{=} p_1 \parallel p_2$, *is as follows:*

$$\frac{\begin{array}{c}\langle A_1, C_1\rangle : \{\varphi_1\}\ p_1\ \{\psi_1\} \\ \langle A_2, C_2\rangle : \{\varphi_2\}\ p_2\ \{\psi_2\} \\ A \wedge C_1 \rightarrow A_2,\ A \wedge C_2 \rightarrow A_1\end{array}}{\langle A, C_1 \wedge C_2\rangle : \{\varphi_1 \wedge \varphi_2\}\ p\ \{\psi_1 \wedge \psi_2\}}\ \begin{array}{l}Parallel\\ Composition\end{array}$$

Where $\langle A, C_1 \wedge C_2\rangle$ are assumptions and commitments of the new process (p), regarding its environment. If A_i $(i \in \{1,\ 2\})$ contains assumptions about the connected channels to both P_1 and P_2, then C_j $(j \in \{1,\ 2\} \wedge j \neq i)$ should justify them. If A_i includes assumptions about the external channels of P_i, the new assumptions A should justify them. Verifying the conditions $A \wedge C_i \rightarrow A_j$ $(i, j \in \{1,\ 2\} \wedge i \neq j))$ leads to verifying the above conditions in p.

2.3 Memory-Driven Computing (MDC)

MDC [35] is a disaggregated-memory architecture. It realizes memory disaggregation as a shared fabric-attached memory pool. PEs and NVM modules connect via bridges

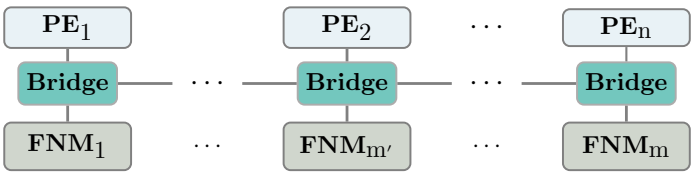


Figure 2: MDC Architecture.
Legend: FNM: Fabric-attached NVM Module

to the fast-speed fabric, as depicted in Figure 2. Near-uniform low latency of optical networking provides memory-speed access time to the NVM modules.

MDC provides distributed heterogeneous computing by enabling general-purpose CPUs and task-specific processors to attach the fabric and read/write (r/w) from/to the shared memory. Bridges route memory read/write requests to corresponding NVM modules, in which memory controllers execute them and return responses. Thus, processes can directly access all the memory addresses.

2.4 Threat Model

This work assumes a threat model where adversaries cannot physically access resource and intermediate controllers or compromise them via the network. Our system use one-way hash function and encryption to make unforgeable capabilities; thus, adversaries cannot forge new capabilities or alter existing ones. Furthermore, we assume architectures preserve the confidentiality and integrity of exchanged data by protecting connections between their elements using existing mechanisms, such as encryption. This threat model has two types of PEs: secured and unsecured. We assume an adversary can compromise any process in unsecured PEs but cannot compromise processes in secured ones. Various attacks, such as side-channel attacks, are out of the scope of this work.

3 Related Work

Following Bresniker et. al. [10] work, we reviewed 18 existing capability systems (Table 1) and compare them.

Methodology. Our methodology comprises two main steps. First, we systematically review existing literature on capability systems (i.e., Table 1), offered features by each one, their use cases, and their requirements. Then, we use the extracted features as qualitative criteria to compare existing systems against one another comprehensively. Table 1 summarizes the reviewed capability systems and the traits they cover, in which ● means that a system fully supports a trait, ◐ indicates a system partially supports a trait, and ○ denotes that a system does not satisfy a trait. The six extracted traits are as follows.

Distributed Structure. This criterion expresses that an access-control system should support a distributed system; thus, it indicates that the system should be scalable without suffering from a single point of failure problem. We refer to a capability system fully distributed if it controls access on resource sides and PE sides and can handle internal delegation locally; we indicate a system partially distributed if it only controls access on the resource sides.

Subject Granularity. This criterion refers to the granularity of subjects a system can recognize in each stage of access control. Process level is the most fine-grained subject granularity. A capability system fully supports fine-grained subject granularity if it can distinguish processes at both PE and resource sides.

Object Granularity. This criterion presents the minimum unit of a resource object that an access-control system can distinguish regarding the resource type. For example, the most fine-grained memory granularity is at the byte level.

Capability Delegation. A process should be able to delegate a subset of its capability privileges to other processes only through authorized channels.

Capability Revocation. A process should be able to revoke a delegated capability and all re-delegated capabilities in its capability-hierarchy.

Persistency. A capability system is persistence if capabilities can outlive their corresponding processes or OS reboots.

The distributed trait is a fundamental demand for disaggregated-resource architectures. Capability persistency is crucial to eliminate security risks because a persistent resource, such as persistent memory, may contain sensitive data, which remains in the resource after rebooting the system. The ability to delegate supports cooperation between processes, while the inability to revoke introduces a security vulnerability. As Table 1 depicts, each system covers 3.38 traits fully and 1.16 ones partially on average. However, nine (50%), sixteen (81%), ten (55%), and eleven (61%) of the systems cover, fully or partially, distributed, delegation, revocation, and persistency traits, respectively; none of them fully covers all the four traits. As we demonstrate in Section 4, our design fully covers all the six traits.

Now, we review capability system in more details by dividing them to Hardware-supported and OS-based systems.

Hardware-supported Systems. *CAP* [52], *StarOS* [32], *IBM System/38* [30], and CHERI [66] extend *instruction set architecture* (ISA) to protect memory in single sys-

Table 1: Capability-based Access-control Systems

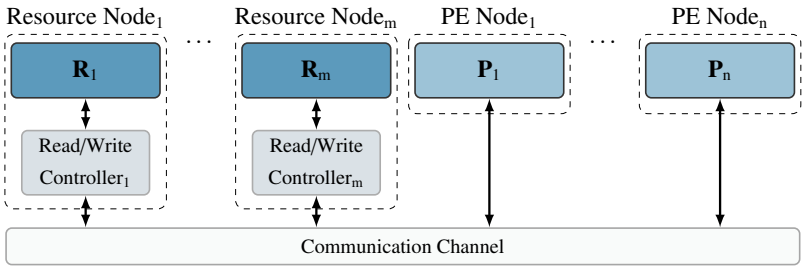
	CAP [52]	StarOS [32]	IBM/38 [30]	Hardbound [19]	iAPX432 [14]	CHERI [66]	M-Machine [12]	Hydra [67]	Chorus [58]	Amoeba [50]	Accent [57]	KeyKOS [26]	Mach [1]	EROS [60]	L4 [40]	Barrelfish [7]	CEP [6]	SemperOS [28]	SADRA
Distributed	○	●	○	○	●	○	○	○	●	●	●	○	●	○	○	●	◐	●	●
Subject Granularity	●	◐	●	●	●	●	●	●	●	●	●	●	●	●	●	●	◐	●	●
Object Granularity	●	●	●	◐	●	●	●	●	◐	◐	◐	◐	◐	◐	◐	◐	●	●	●
Capability Delegation	●	●	●	○	○	●	●	●	●	●	◐	●	●	●	●	●	●	●	●
Capability Revocation	○	○	●	○	○	○	●	○	●	◐	◐	○	◐	●	○	●	●	◐	●
Persistency	●	○	○	○	●	○	●	○	◐	●	○	◐	◐	●	●	○	●	◐	●
HW/SW Demands	ISA/OS	ISA/OS	ISA	ISO/C	ISA	ISA/C	HW/ISA	OS	OS	OS	OS	OS	OS	OS	OS	OS	Co-P	HW/OS	Co-P

Legend: ●=fully; ◐=partially; ○=no
C: Compiler; Co-P: Co-Processor; ISA: Instruction Set Architecture; OS: Operating System

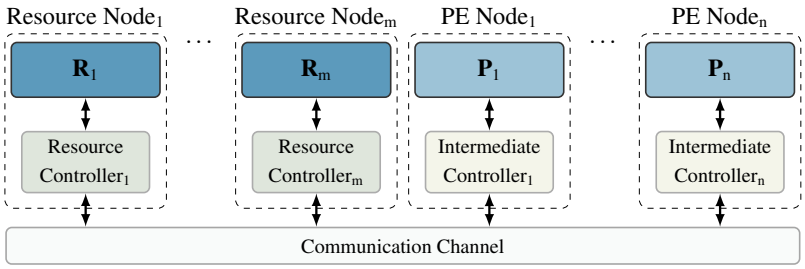
tems. CAP proposes a hardware design cand an associated operating system to manage capabilities. IBM System/38 implement capabilities as pointers and protect them with tags bits. Users can pass the capabilities but cannot change their tags' value. CHERI proposed a hybrid capability model using a capability co-processor and tagged memory. Contrary to our system, these system are non-distributed ones.

StarOS is a distributed object-oriented system based on *Cm** architecture[62]. CEP [6] presents a distributed memory controller, implemented via co-processors.Because CEP only manages access on the memory side, it introduces communication overhead and is vulnerable to DoS attacks. Furthermore, handling local delegation/revocation operations between two processes requires communication with remote controllers. SemperOS [28] proposes a multi-kernel OS based on a hardware element, namely *data transfer unit* (DTU). It divides PEs into groups and controls each group via an independent kernel, in which kernels communicate by passing messages using DTUs. Furthermore, SemperOS assigns every PE's capabilities statically because it does not support migrating new PEs due to its capability-addressing scheme. Kernels collaborate to handle capability-related operations, which causes communication overhead and makes a system vulnerable to DoS attacks during revoking capability hierarchies. SemperOS allows spawning at most two threads per kernel to mitigate the vulnerability.

OS-based Systems. *HYDRA* [67] is an OS that treats capabilities as references to resources and allows only the kernel to manipulate them. *KeyKOS* [26], *Accent* [57], *Mach* [1], and *EROS* [60] enforce capabilities via micro-kernels. KeyKOS divides a system into domains and employs capabilities to control message passing between them. Accent proposes a distributed communication-oriented OS and provides processes with capabilities to employ communication channels. EROS provides persistent memory access at a page level. A reference monitor mediates process communication and provides transparent delegation/revocation via forwarding objects. Mach [1] is an object-oriented OS that enables processes to pass data and capabilities via a messaging system.



(a) Abstract Disaggregated System.



(b) Distributed Access-control System.

Figure 3: Distributed Systems.

4 Proposed Access-Control System

We introduce the design of our capability-based access-control system in this section. We first present an abstract model for disaggregated systems; then, we introduce *access controller*s and integrate them into this model; finally, we demonstrate our capability model.

4.1 Abstract Disaggregated System

We construct an abstract disaggregated-system model to focus on the general characteristics of disaggregated systems. The model comprises *resource nodes* ($\mathbb{N}_r$), *PE nodes* ($\mathbb{N}_p$), resources ($\mathbb{R}$), *processes* ($\mathbb{P}$), and a *communication medium*, as illustrated in Figure 3a. Each resource node $N_r^j \in \mathbb{N}_r$ $(1 \leqslant j \leqslant m)$ contains a subset of resources $R_j \subseteq \mathbb{R}$, and each PE node $N_p^k \in \mathbb{N}_p$ $(1 \leqslant k \leqslant n)$ hosts a subset of processes $P_k \subseteq \mathbb{P}$. A resource node operates autonomously from other resource nodes. It contains a controller which handles r/w requests. Processes and controllers communicate using the request/response pattern, exchanging messages via the medium. We designed our access-control system based on this model.

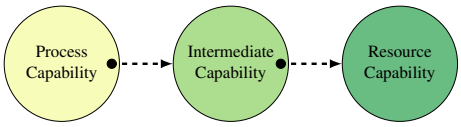


Figure 4: The Capability Model.

4.2 Access Controllers

Imagine a resource node as a country's capital and all the PE nodes as provinces. The central governor delegates a subset of its power to local governors. It only controls access to the capital's resources or handles the relationship between two citizens from different provinces. Hence, the model distributes the central government's workload and reduces the exchanged messages between central and provincial governors. We followed such a model to design a scalable distributed access-control system.

To adapt the model, we designed two controller types: *resource* and *intermediate controllers*, as illustrated in Figure 3b. Resource controller $RC_j \in \mathbb{RC}$ $(1 \leqslant j \leqslant m)$ acts as the central governor in resource node N_r^j, and each intermediate controller $IC_k \in \mathbb{IC}$ $(1 \leqslant k \leqslant n)$ serves as the local governor in PE node N_p^k. Neither resource nor intermediate controllers interact with the controllers of their types. In addition, processes cannot directly communicate with resource nodes or share their access rights with others.

Intermediate controllers handle two main tasks. First, they perform the first stage of access control by inspecting requests and checking if the process possesses the appropriate access rights, regarding their requests. They deny requests if checking fails. Second, they handle local delegation/revocation requests. For example, assume two processes, p, $p' \in P_k$, where p can access resource $r \in R_j$ and wants to share this privilege with p'. Controller IC_k performs the delegation without involving RC_j.

Resource controllers fulfill three main tasks: *allocating resources*, *delegating/revoking access rights*, and *enforcing access rights*. They assign each resource in their nodes to a specific process by performing the first task. Furthermore, they enable access-right delegation/revocation when delegator and receiver processes run in different PE nodes. For example, assume $p \in P_k$ requests to share its access rights to resource $r \in R_j$ with $p' \in P_{k'}$. Resource controller RC_j handles the request, cooperating with intermediate controllers IC_k and $IC_{k'}$. Moreover, they perform the second stage of access control. In the previous example, RC_j declines p''s requests regarding resource r if process p has revoked the permission. Controllers employ the capability tokens to execute their tasks.

4.3 Capability Model

We desire our capability model to reflect the delegated control mechanism between resource and intermediate controllers. Intermediate controllers prevent processes from contacting resource controllers directly; thus, resource controllers only accept requests from intermediate controllers. Now that we have designed our access controllers, we introduce our capability-object model

Our capability model comprises three capability types: *resource* ($\mathbb{C}_r$), *intermediate*

($\mathbb{C}_i$), and *process* ($\mathbb{C}_p$) capabilities, as depicted in Figure 4. As the naming suggests, each type belongs to its corresponding controller/process in our design and contains information about the access rights of a specific process to a particular resource. In addition, process and intermediate capabilities include a pointer, pointing to their corresponding intermediate and resource capabilities. We use operator $\mapsto$ to represent the point-to relation between two capabilities. For example, assume that capabilities $c_p \in \mathbb{C}_p$, $c_i \in \mathbb{C}_i$, and $c_r \in \mathbb{C}_r$, where c_p and c_i point to c_i ($c_p \mapsto c_i$) and c_r ($c_i \mapsto c_r$), respectively. These three capabilities contain the same permissions to access resource $r \in R_j$.

Indicator Flag. A process must indicate the exact delegated capability when it intends to revoke the capability. Thus, our access-control system requires a mechanism to track delegated capabilities; it provides the mechanism using a boolean flag, namely *indicator*, inside capabilities. When the flag is set, the containing capability points to a delegated capability. We refer to a capability when its indicator flag is set simply as an **indicator** and clarify how our system leverages it when explaining capability-related operations (Section 4.3.2). It is worth noting that processes and controllers cannot employ indicators for read/write operations.

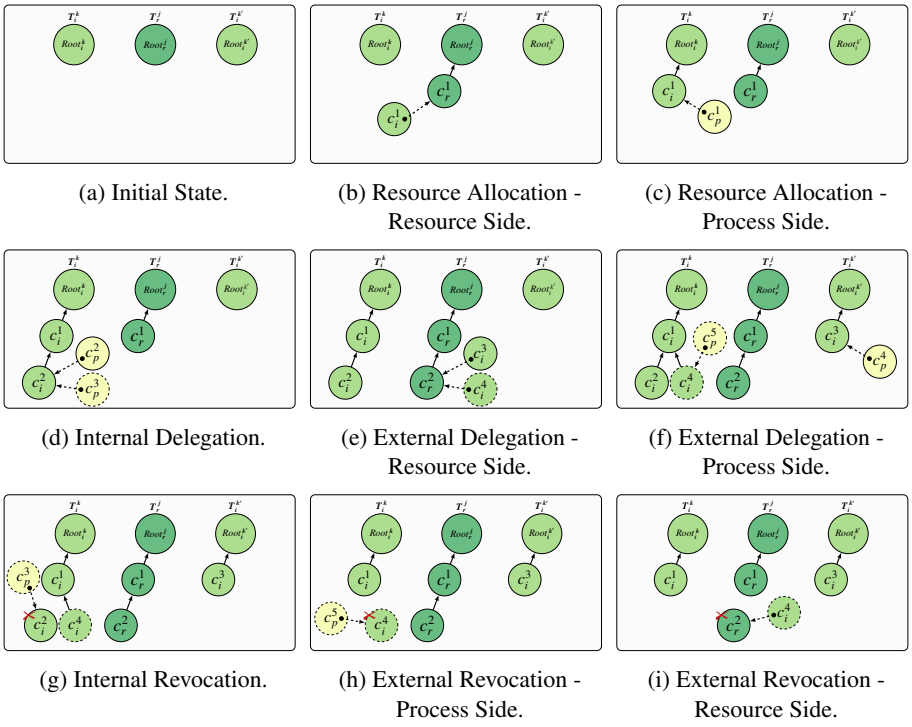
4.3.1 Capability Tree

Controllers preserve their capabilities inside *rooted tree*s [53]. A rooted tree is a tree with a particular vertex as its *root*. We refer to the trees as *capability tree*s ($\mathbb{T}_r \cup \mathbb{T}_i$), where the root capabilities belong to controllers. A subtree in a capability tree represents a *delegation hierarchy* in which a child node indicates a delegation from its parent capability. A controller only possesses the authority to add/remove capabilities to/from its tree and leverages it to handle capability-related operations. Controllers retain their trees in Non-Volatile memories. It enables controllers to support capability persistency.

4.3.2 Capability-related Operations

Capability-related operations include allocating resources and delegating/revoking capabilities. We demonstrate how controllers leverage capability trees to accomplish their tasks through an example. Imagine a disaggregated system where process $p \in P_k$ requests gaining *read/write* (r/w) access to resource $r \in R_j$ (*resource allocation*). After gaining access, p delegates the received privileges to process $p' \in P_k$ in the same PE node (*internal delegation*) and process $p'' \in P_{k'}$ in another PE node (*external delegation*). Finally, process p revokes both delegated capabilities (*internal* and *external revocation*). **??** 4.3.1–5i illustrate how the controllers modify their capability trees to accomplish their tasks in the above scenario. The controllers' trees contain only their root capabilities at the initial state, as depicted in Section 4.3.1.

Resource Allocation. By receiving the request, resource controller RC_j allocates the resource and creates a resource capability, c_r^1, which comprises data about p and r. Then, it inserts the capability as the root's child inside its tree and forges the corresponding intermediate capability, c_i^1, as illustrated in Figure 5b. To complete its task, controller RC_j sends c_i^1 to intermediate controller IC_k.



(a) Initial State. (b) Resource Allocation - Resource Side. (c) Resource Allocation - Process Side.

(d) Internal Delegation. (e) External Delegation - Resource Side. (f) External Delegation - Process Side.

(g) Internal Revocation. (h) External Revocation - Process Side. (i) External Revocation - Resource Side.

Figure 5: Capability Trees.
Legend: ○ = process capability; ○ = intermediate capability; ● = resource capability
○ = indicator flag is unset; ◌ = indicator flag is set;
●- - -►: pointed-to connection in our capability-object model; ⟶: child-parent relation in a capability tree

The Intermediate Controller adds the received capability to its capability tree (Figure 5c). Furthermore, IC_k forges the corresponding process capability, c_p^1, and sends it to process p. Hence, p possesses an unforgeable process capability.

Internal Delegation. Control IC_k handles delegating the capability to p' because both processes run on the same node. The controller generates intermediate capability c_i^2 and inserts it as the child of capability c_i^1 by receiving the request (Figure 5d). Furthermore, the controller forges the corresponding process capability, c_p^2, and sends it to p'. Process p' can now employ the received capability to execute r/w operations over resource r. Moreover, controller IC_k forges indicator c_p^3 for p. Process p can employ the indicator to revoke the delegated capability; however, it can neither apply the indicator during r/w requests nor re-delegate it.

External Delegation. Intermediate controller IC_k collaborates with resource controller RC_j to handle the external delegation. Controller RC_j generates and inserts resource capability c_r^2 to its tree due to the request (Figure 5e). Furthermore, RC_j forges

intermediate capability c_i^3 for controller $IC_{k'}$ and indicator c_i^4 for controller IC_k.

Both intermediate controllers add the received capabilities to their trees (Figure 5f). Controller $IC_{k'}$ creates process capability c_p^4 for process p'', and controller IC_k forges indicator c_p^5 for process p. At this stage, processes p, p', and p'' possess the capability sets $\{c_p^1,\ c_p^3,\ c_p^5\}$, $\{c_p^2\}$, and $\{c_p^4\}$, respectively.

Internal Revocation. Process p leverages indicator c_p^3 to revoke the delegated capability to process p'. When intermediate controller IC_k receives the request, it realizes that the indicator points to intermediate capability c_i^2 inside its tree (Figure 5g). Hence, the controller performs an internal revocation only by removing capability c_i^2 from its tree. Process p' cannot use process capability c_p^3 any further because the process capability points to a non-existing intermediate capability in the capability tree.

External Revocation. Process p employs indicator c_p^5 to revoke the delegated capability to p''; by receiving the revocation request, controller IC_k notices that the indicator points to another indicator, c_i^4, in its tree. Hence, the controller removes indicator c_i^4 from its tree at the first phase (Figure 5h). Afterward, the controller forwards the request along with indicator c_i^4 toward resource controller RC_j.

When controller RC_j receives the request, it notices that indicator c_i^4 points to capability c_r^2 inside its capability tree. The controller removes capability c_r^2 from its tree (Figure 5i), which completes the external revocation.

At this stage, the p'''s request, comprising process capability c_p^4, to read/write from/to resource r passes the first access check at controller $IC_{k'}$ because c_p^4 points to an existing intermediate capability, c_i^3, inside the controller's tree. Thus, controller $IC_{k'}$ forwards the request along with c_i^3 to resource controller RC_j. However, controller RC_j returns a failure response to $IC_{k'}$ because c_i^3 points to capability c_r^2, which no longer exists in the controller's tree. Consequently, intermediate controller $IC_{k'}$ removes capability c_i^3 from its tree and forwards the failure response to process p''.

5 System Design's Soundness

Now that we have seen how our system controls access, we prove that our capability-based access control system is sound. Following Maffeis et al. [44] work, we prove our system design's soundness by demonstrating that it satisfies the capability-safety and authority-safety properties. Furthermore, we prove that our system guarantees isolation property based on these two properties.

In the rest of the section, we employ a few auxiliary functions in the definitions and proofs. Table 2 lists the functions and their descriptions, in which $\mathbb{V} = \{r, w\}$ is the permission set (r: read, w: write), and $\mathbb{R}$ denotes the set of all resources.

5.1 Well-Formed Capability Trees

To define well-formed capability trees, we must first specify the partial order.

Partial Order. We define the partial order ($\prec$) between two capabilities ($c' \prec c$) as follows:

$$c' \prec c \iff rsrc(c') \subseteq rsrc(c) \ \wedge \ priv(c') \subseteq priv(c)$$

We use the partial-order property to specify the relation between capabilities in a delegation hierarchy.

Resource-capability Tree. A resource-capability tree $T_r \in \mathbb{T}_r$ is a rooted tree with the root $c_r^{root} \in \mathbb{C}_r$. The root capability belongs to the resource controller, points to all the node's resources, and possesses all the permissions. The controller generates no corresponding intermediate capability for it. Tree T_r is a well-formed resource-capability tree if all its sub-trees are partially-ordered delegation hierarchy as follows:

$$\forall c_r,\ c_r' \in \mathbb{C}_r : isInTree(T_r,\ c_r,\ c_r') \Rightarrow c_r' \prec c_r$$

Theorem 5.1. *A well-formed resource tree $T_r \in \mathbb{T}_r$ remains well-formed after performing capability-related operations.*

Proof. The proof proceeds by structural induction on T_r and comprises a base case and three inductive cases.

- **Base Case:** T_r only contains the root capability.
  In this case, the tree satisfies the well-formness' condition.
- **Inductive Case One:** T_r is a well-formed capability tree, and the resource controller (RC) allocates a resource.
  After allocating the resource, RC forges the corresponding capability (c_r) for it such that $c_r \prec c_r^{root}$; then, RC inserts it to T_r as the child of the root. Hence, the resource-allocating exercise retains the tree's well-formedness.
- **Inductive Case Two:** T_r is a well-formed capability tree, and RC performs an external capability-delegation operation over c_r.
  RC delegates c_r by constructing c_r' such that $c_r' \prec c_r$. Afterward, RC adds c_r' into

T_r as the child of c_r. Thus, the external-delegating operation preserves the tree's well-formedness.

- **Inductive Case Three:** T_r is a well-formed capability tree, and *RC* performs an external capability-revocation operation over c_r.
  RC removes c_r and all the capabilities in its subtree. Thus, the external-revocation operation preserves the tree's well-formedness.

□

Intermediate-capability Tree. An intermediate-capability tree $T_i \in \mathbb{T}_i$ is a rooted tree with the root $c_i^{root} \in \mathbb{C}_i$. The root capability belongs to the intermediate controller, but it points to no resource and possesses no permissions; thus, the controller generates no corresponding process capability for it. Tree T_i is a well-formed intermediate-capability tree if all its sub-trees (not including the root) are partially-ordered delegation hierarchy as follows:

$$\forall\, c_i, c_i' \in \mathbb{C}_i : \mathit{isInTree}(T_i,\, c_i,\, c_i') \,\wedge\, \neg \mathit{isRoot}(T_i,\, c_i) \Rightarrow c_i' \prec c_i$$

Theorem 5.2. *A well-formed intermediate tree $T_i \in \mathbb{T}_i$ remains well-formed after performing capability-related operations.*

Proof. The proof proceeds by structural induction on T_i and comprises a base case and three inductive cases.

- **Base Case:** T_i only contains the root capability.
  In this case, the tree satisfies the well-formness' condition.
- **Inductive Case One:** T_i is a well-formed capability tree, and the resource controller (*IC*) receives an intermediate capability or an indicator due to a resource allocation or an external delegation, respectively. *IC* inserts the received capability or indicator to T_i as the child of the root. Hence, allocating resource or externally delegating a capability retain the tree's well-formedness.
- **Inductive Case Two:** T_i is a well-formed capability tree, and *IC* performs an internal capability-delegation operation over c_i.
  IC delegates c_i by constructing c_i' such that $c_i' \prec c_i$. Afterward, *IC* adds c_i' into T_i as the child of c_i. Thus, the internal-delegating operation preserves the tree's well-formedness.
- **Inductive Case Three:** T_i is a well-formed capability tree, and *IC* performs an internal capability-revocation operation over c_i.
  IC only removes c_i and all the capabilities in its subtree. Thus, the internal-revocation operation preserves the tree's well-formedness.

□

Table 2: Function Definitions

Function Name	Function Signature	Description
rsrc	$\mathbb{C} \rightarrow \mathbb{R}$	returns the pointed resources inside a capability.
priv	$\mathbb{C} \rightarrow 2^{\mathbb{V}}$	returns the permissions inside a capability
getRoot	$\mathbb{T}_x \rightarrow \mathbb{C}_x$	returns the root of a capability tree.
isRoot	$\mathbb{T}_x \times \mathbb{C}_x \rightarrow boolean$	checks if a capability is the root of a capability tree
isInTree	$\mathbb{T}_x \times \mathbb{C}_x \times \mathbb{C}_x \rightarrow boolean$	checks if the second capability is inside a tree, where the first capability indicates the search's start point.

Legend: $x \in \{r,\ i\}$, $\mathbb{C} = \{\mathbb{C}_r \cup \mathbb{C}_i \cup \mathbb{C}_p\}$

5.2 Valid Capability

A capability is valid if the capability owner can employ it to execute read/write operations over the pointed resource by the capability. Because an intermediate controller or a process can send a request, we demonstrate the validity of a capability at both levels.

5.2.1 Valid Intermediate Capability

An intermediate capability is valid if a resource controller has forged it and it points to an existing resource capability inside the controllers tree. For example, consider capabilities c_i^1 and c_i^3 in Figure 5i. c_i^1 points to an existing capability (c_r^1) inside T_r^j. Hence, IC_k can employ it to exercise the read/write operations, which makes c_i^1 a valid capability. At the same time, c_i^3 is an invalid capability because it points to a removed resource capability (c_r^2) from T_r^j. We formally define a valid intermediate capability as follows:

$$
\begin{aligned}
isValidIntCap(c_i) \stackrel{\text{def}}{=}\ & \exists\, c_r \in \mathbb{C}_r,\ T_r \in \mathbb{T}_r : \\
& c_i \mapsto c_r \wedge \\
& isInTree(T_r,\ getRoot(T_r),\ c_r)
\end{aligned}
$$

Resource controllers can only forge valid intermediate capabilities or invalidate them by removing the pointed resource capabilities from their trees.

5.2.2 Valid Process Capability

A process capability is valid if it points to an existing resource capability inside a resource controller's tree. In addition, the pointed intermediate capability must be valid or be in the delegation hierarchy of a valid one. We denote the capability on top of a delegation hierarchy as an *original* intermediate capability. It means a resource controller has forged the capability with an unset indicator flag. Let $(S^i,\ c_i)$ be a rooted subtree of (T_i, c_i^{root}), in which node c_i denotes the subtree's root and is the child of c_i^{root}.

Subtree S^i indicates a delegation hierarchy inside T_i. Capability c_i is original, while the rest of the capabilities in S^i are not. For example, consider capabilities c_i^1 and c_i^2 inside tree T_i^k in Figure 5d. c_i^1 is an original capability while c_i^2 is not.

Resource controllers only accept original intermediate capabilities for read/write operations because they have forged them and can check their integrity. In the above example, suppose process p employs c_p^2 to read from resource r. Although c_p^2 points to c_i^2, IC_k cannot replace c_p^2 with c_i^2 when it forwards the request to RC_j. Instead, IC_k first replaces c_p^2 with c_i^1 as it is the original capability of c_i^2; then, IC_k forwards the request.

We define function **getOriginalCap**: $\mathbb{T}_i \times \mathbb{C}_i \rightarrow \mathbb{C}_i$ to find an original capability inside an intermediate-capability tree. The function traverses the tree from a given capability toward the root until it reaches an original capability in the path. We formally define a valid process capability as follows:

$$
\begin{aligned}
isValidProCap(c_p) \stackrel{\text{def}}{=} \exists\, c_i,\ c_i' \in \mathbb{C}_i,\ T_i \in \mathbb{T}_i :\\
c_p \mapsto c_i \wedge\\
isInTree(T_i,\ getRoot(T_i),\ c_i) \wedge\\
c_i' = getOriginalCap(T_i,\ c_i) \wedge\\
isValidIntCap(c_i')
\end{aligned}
$$

For instance, in Figure 5h, c_p^4 is a valid capability while c_p^5 is not because IC_k has removed c_i^4 from its capability tree. Now that we have expressed the well-formed capability trees and specified valid capability, we define the security properties.

5.3 Security Properties

Our access-control system guarantees three security properties, including: *capability safety*, *authority safety*, and *isolation*. We prove our system satisfies these properties by demonstrating that our design handles capability-related operations correctly; thus, we first define five lemmas, one for each operation, and verify them using the assumption-commitment technique.

Our modeling has three component types: *process*, *resource controller*, and *intermediate controller*. In this modeling, the components interact to execute an operation. We consider five operations in this modeling: resource allocation, internal capability delegation, external capability delegation, internal capability revocation, and external capability revocation. In addition, we define five lemmas based on the operations and explain the operations' precondition, postcondition, assumption, and commitment properties to prove the lemmas based on the assumption-commitment (A-C) technique. Each proof considers the states of the components involved in the corresponding operation.

5.4 First Lemma: Resource Allocation

The first lemma indicates that any resource-allocation operation creates a valid p-cap. We formally define the lemma and proof it.

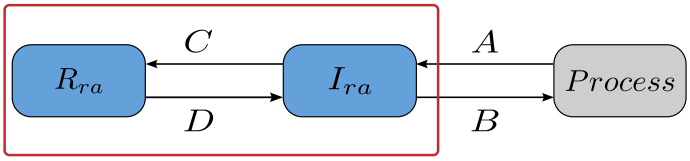


Figure 6: Syntactic Interfaces of the Resource-allocation Programs.

Lemma 1. *Given a process with a unique PID in a process node with a unique NID, an intermediate controller in the same node, and an resource controller in a resource node with a unique NID, the process will get a valid p-cap by sending a resource-allocation request.*

Proof. We use the assumption-commitment technique to prove the lemma.

To prove the lemma, we model the intermediate and the resource controllers in a resource-allocation operation by programs $I_{ra} \stackrel{\text{def}}{=} (L^i_{ra}, T^i_{ra}, s^i_{ra}, t^i_{ra})$ and $R_{ra} \stackrel{\text{def}}{=} (L^r_{ra}, T^r_{ra}, s^r_{ra}, t^r_{ra})$, respectively. The programs and the process exchange messages via synchronous channels to handle resource-allocation requests. Figure 6 depicts these two programs and their syntactic interfaces. In addition, figures 7a and 7b illustrate sequential diagrams of programs I_{ra} and R_{ra}, respectively. In the next step, we prove that when the process sends a resource-allocation request, it will receive a valid p-cap.

5.4.1 Resource Allocation - Intermediate Controller

Program I_{ra} receives a resource-allocation request from the process via channel A, creates a corresponding request for program R_{ra}, and sends it through channel C. Furthermore, It receives the response from program R_{ra} via channel D. Program I_{ra} updates its capability tree when it receives an i-cap from the resource controller by inserting the capability inside the tree. In addition, it creates the corresponding p-cap for the inserted i-cap. Finally, it creates a response for the process and sends the p-cap inside the response to the process through channel B. The functions of I_{ra} are as follows:

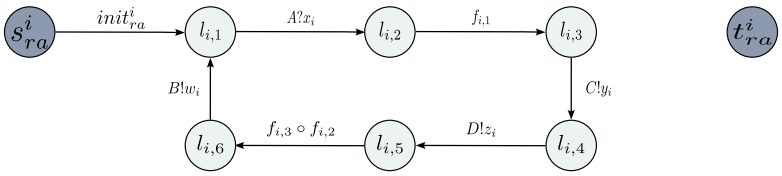
$$
\begin{aligned}
init^i_{ra}(\sigma) &= (\sigma : rootPtr \mapsto getRoot(\sigma(T_i))),\\
f_{i,1}(\sigma) &= (\sigma : y_i \mapsto genRaReq(\sigma(x_i))),\\
f_{i,2}(\sigma) &= (\sigma : pCap \mapsto insert(\sigma(rootPtr), \sigma(z_i.cap)))\\
f_{i,3}(\sigma) &= (\sigma : w_i \mapsto genRaRes(\sigma(x_i), \sigma(pCap)))
\end{aligned}
$$

The A-C formula for program I_{ra} is as follows:

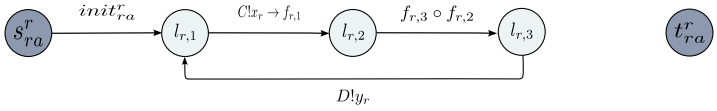
$$\vdash \langle Ass^i_{ra},\ C^i_{ra}\rangle\ \{\varphi^i_{ra}\}\ I_{ra}\ \{\psi^i_{ra}\}$$

where the formal definition of φ^i_{ra}, ψ^i_{ra}, Ass^i_{ra}, and C^i_{ra} are as follows:

$$
\begin{aligned}
\varphi^i_{ra} &\stackrel{\text{def}}{=} \#A = \#B = \#C = \#D = 0\ \wedge\ |icTree| \geqslant 1\\
\psi^i_{ra} &\stackrel{\text{def}}{=} false
\end{aligned}
$$



(a) Program I_{ra}.



(b) Program R_{ra}.

Figure 7: Resource-allocation Programs.

$$
\begin{aligned}
Ass^i_{ra} \quad &\stackrel{\text{def}}{=} \quad (\#A > 0 \rightarrow \\
&\qquad isRaReq(last(A)) \ \wedge \ isUniquePID(last(A).spid)) \wedge \\
&\quad (\#C = \#D > 0 \rightarrow \\
&\qquad isRaRes(last(D)) \ \wedge \ isValidCap(last(D).cap)) \\
C^i_{ra} \quad &\stackrel{\text{def}}{=} \quad (\#A = \#B = \#C = \#D > 0 \rightarrow \\
&\qquad isRaRes(last(B)) \ \wedge \ isValidCap(last(B).cap))) \wedge \\
&\quad (\#C > 0 \rightarrow \\
&\qquad isRaReq(last(C)) \ \wedge \ isUniquePID(last(C).spid)))
\end{aligned}
$$

Wherein $icTree$ is the capability tree of the intermediate controller.

The assertion network for I_{ra} is as follows:

$$
\begin{aligned}
Q_{s^i_{ra}} &\stackrel{\text{def}}{=} \#A = \#B = \#C = \#D = 0 \ \wedge \ |T_i| \geqslant 1 \\
Q_{l_{i,1}} &\stackrel{\text{def}}{=} \#A = \#B = \#C = \#D \\
Q_{l_{i,2}} &\stackrel{\text{def}}{=} \#B = \#C = \#D = (\#A - 1) \ \wedge \ last(A) = x_i \wedge \\
&\qquad isRaReq(last(A)) \ \wedge \ isUniquePID(last(A).spid) \\
Q_{l_{i,3}} &\stackrel{\text{def}}{=} \#B = \#C = \#D = (\#A - 1) \ \wedge \ last(A) = x_i \wedge \\
&\qquad isRaReq(y_i) \ \wedge \ isUniquePID(y_i.spid) \\
Q_{l_{i,4}} &\stackrel{\text{def}}{=} \#B = \#D = (\#A - 1) = (\#C - 1) \ \wedge \ last(A) = x_i \wedge \\
&\qquad last(C) = y_i \\
Q_{l_{i,5}} &\stackrel{\text{def}}{=} \#A = \#C = \#D = (\#B + 1) \ \wedge \ last(A) = x_i \wedge \\
&\qquad last(C) = y_i \ \wedge \ last(D) = z_i \ \wedge \ isRaRes(last(D)) \wedge \\
&\qquad isValidCap(last(D).cap)
\end{aligned}
$$

$$Q_{l_{i,6}} \stackrel{\text{def}}{=} \#A = \#C = \#D = (\#B + 1) \ \wedge \ last(A) = x_i \ \wedge$$
$$last(C) = y_i \ \wedge \ last(D) = z_i \ \wedge$$
$$isRaRes(w_i) \ \wedge \ isValidCap(w_i.cap)$$
$$Q_{t^i_{ra}} \stackrel{\text{def}}{=} false$$

We check the following implications to prove that the above assertion network is an A-C-inductive assertion network w.r.t. assumption A^i_{ra}, commitment C^i_{ra}, and channels A, B, C, and D.

- $\models Q_{s^i_{ra}} \rightarrow C^i_{ra}$ follows from the above definitions.
- $\models Q_{s^i_{ra}} \wedge A^i_{ra} \rightarrow Q_{l_{i,1}} \circ init^i_{ra}$. In this internal transition, the size of the intermediate-capability tree does not change. Hence, this verification holds.
- $\models Q_{l_{i,1}} \ \wedge \ A^i_{ra} \ \rightarrow ((A^i_{ra} \ \rightarrow \ Q_{l_{i,2}}) \ \wedge \ C^i_{ra}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x_i, \ h \mapsto v, \ \sigma(h).(A, v))$ for arbitrary value v. In this input transition, just communication through channel A took place, and function g assigns the received value to x_i. Because $\#A > 0$, the first implication of Ass_i satisfies $isRaReq(last(A))$ and $isUniquePID(last(A).spid)$. Thus, this verification holds.
- $\models Q_{l_{i,2}} \ \wedge \ A^i_{ra} \ \rightarrow \ Q_{l_{i,3}} \circ f_{i,1}$. In this internal transition, function $f_{i,1}$ creates a resource-allocation request for program R_{rr} and assigns it to variable y_i, such that $isRaReq(y_i) = true$ and $y_i.spid = last(A).spid$. In addition, $\sigma' \models isUniquePID(y_i.spid)$ because , from A^i_{ra}, we have $isUniquePID(last(A).spid) = true$. Thus, this verification holds.
- $\models Q_{l_{i,3}} \wedge A^i_{ra} \rightarrow ((A^i_{ra} \rightarrow Q_{l_{i,4}}) \wedge C^i_{ra}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(C, \sigma(y_i)))$. In this output transition, program I_{ra} sends y_i through channel C. C^i_{ra} holds because $last(C) = \sigma(y_i)$ and $\sigma \models isRaReq(y_i) \wedge isUniquePID(y_i.spid)$. Hence, this verification holds.
- $\models Q_{l_{i,4}} \wedge A^i_{ra} \rightarrow ((A^i_{ra} \rightarrow Q_{l_{i,5}}) \wedge C^i_{ra}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : z_i, h \mapsto v, \sigma(h).(D, v))$ for arbitrary value v. In this input transition, a communication through channel D just took place, and function g assigns the received value to z_i. Since $\#D > 0$, from A^i_{ra} we have $\sigma' \models isRaRes(z_i) \ \wedge \ isValidCap(z_i.cap)$ Thus, this verification holds.
- $\models Q_{l_{i,5}} \wedge A^i_{ra} \rightarrow Q_{l_{i,6}} \circ (f_{i,3} \circ f_{i,2})$. In this internal transition, function $f_{i,2}$ inserts the intermediate capability $iCap$ into T_i and returns $pCap$ that points to $iCap$ inside the tree. Hence, $\sigma' \models |T_i| > 1$. Because $\sigma \models isValidCap(iCap)$ and $pCap$ points to the inserted $iCap$ inside T_i, we have $\sigma' \models isValidCap(pCap)$. Function $f_{i,3}$ creates a response for the process and assigns it to w_i, wherein $w_i.cap = pCap$. Consequently, $\sigma' \models isRaRes(w_i) \ \wedge \ isValidCap(w_i.cap)$. Thus, this verification holds.
- $\models Q_{l_{i,6}} \wedge A^i_{ra} \rightarrow ((A^i_{ra} \rightarrow Q_{l_{i,1}}) \wedge C^i_{ra}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B, \sigma(w_i)))$. In this output transition, program I_{ra} sends w_i through channel B. C^i_{ra} holds because $\sigma \models isRaRes(w_i) \ \wedge \ isValidCap(w_i.cap)$. Hence, this verification holds.

Since $Q_{t^i_{ra}} \rightarrow \psi^i_{ra}$, the post-condition of program I_{ra} is satisfied.

5.4.2 Resource Allocation - Resource Controller

Program R_{ra} receives a request for allocating a resource from program I_{ra} via channel C. In the next step, program R_{ra} allocates the requested resource and inserts its corresponding resource capability inside its capability tree. Furthermore, it creates the corresponding intermediate capability of the resource capability. Finally, program R_{ra} creates a response, inserts the intermediate capability, and sends the response message through channel D toward program I_{ra}. The conditions and functions of R_{ra} are as follows:

$$
\begin{aligned}
init^{r}_{ra}(\sigma) &= (\sigma : rootPtr \mapsto getRoot(\sigma(T_r))),\\
f_{r,1}(\sigma) &= (\sigma : rCap \mapsto allocRes(\sigma(x_r))),\\
f_{r,2}(\sigma) &= (\sigma : iCap \mapsto insert(\sigma(T_r), \sigma(rootPtr),\\
&\qquad \sigma(rCap))),\\
f_{r,3}(\sigma) &= (\sigma : y_r \mapsto genRaRes(\sigma(x_r), iCap))
\end{aligned}
$$

where T_r is the resource-capability tree, $rCap$ is a resource capability , and $iCap$ is an intermediate capability.

The A-C formula for process R_{ra} is as follows:

$$\vdash \langle A^{r}_{ra}\ C^{r}_{ra}\rangle\ \{\varphi^{r}_{ra}\}\ R_{ra}\ \{\psi^{r}_{ra}\}$$

where the formal definition of φ^{r}_{ra}, ψ^{r}_{ra} , A^{r}_{ra}, and C^{r}_{ra} are as follows:

$$
\begin{aligned}
\varphi^{r}_{ra} &\stackrel{\text{def}}{=} \#C = \#D = 0\ \wedge\ |T_r| = 1\\
\psi^{r}_{ra} &\stackrel{\text{def}}{=} false\\
A^{r}_{ra} &\stackrel{\text{def}}{=} \#C > 0 \rightarrow\\
&\qquad (isRaReq(last(C))\ \wedge\ isUniquePID(last(C).spid))\\
C^{r}_{ra} &\stackrel{\text{def}}{=} (\#C = \#D > 0) \rightarrow\\
&\qquad (isRaRes(last(D))\ \wedge\ isValidCap(last(D).cap))
\end{aligned}
$$

The assertion network for R_{ra} is as follows:

$$
\begin{aligned}
Q_{s^{r}_{ra}} &\stackrel{\text{def}}{=} \#C = \#D = 0\ \wedge\ |T_r| = 1\\
Q_{r_1} &\stackrel{\text{def}}{=} \#C = \#D\\
Q_{r_2} &\stackrel{\text{def}}{=} \#D = (\#C - 1)\ \wedge\ last(C) = x_r\ \wedge\ isRaReq(last(C)) \wedge\\
&\qquad isUniquePID(last(C).spid)\ \wedge\ isValidCap(rCap)\\
Q_{r_3} &\stackrel{\text{def}}{=} \#D = (\#C - 1)\ \wedge\ last(C) = x_r \wedge\\
&\qquad isRaRes(y_r)\ \wedge\ isValidCap(y_r.cap)\\
Q_{t^{r}_{ra}} &\stackrel{\text{def}}{=} false
\end{aligned}
$$

We check the following implications to prove that the above assertion network is an A-C-inductive assertion network w.r.t. assumption A^r_{ra}, commitment C^r_{ra}, and channels C and D.

- $\models Q_{s^r_{ra}} \rightarrow C^r_{ra}$ follows from the above definitions.
- $\models Q_{s^r_{ra}} \wedge A^r_{ra} \rightarrow Q_{l_{r,1}} \circ init^r_{ra}$. In this internal transition, the size of the capability tree does not change. Hence, this verification holds.
- $\models Q_{l_{r,1}} \wedge A^r_{ra} \rightarrow ((A^r_{ra} \rightarrow Q_{l_{r,2}}) \wedge C^r_{ra}) \circ (f_{r,1} \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x_r,\ h \mapsto v,\ \sigma(h).(C, v))$ for arbitrary v. In this input transition, a communication through channel C just took place. Function g assigns the last received value from channel C to x_r. Since $\#C > 0$, the first implication of A^r_{ra} satisfies $isRaReq(last(C))$ and $isUniquePID(last(C).spid)$ predicates. Function $f_{r,1}$ allocates the requested resource and assigns the returned valid r-cap to $rCap$. Hence, Q_{r_2} satisfies $isValidCap(rCap)$ predicate. C^r_{ra} holds since $\#C \neq \#D$. Thus, this verification holds.
- $\models Q_{l_{r,2}} \wedge A^r_{ra} \rightarrow Q_{l_{r,3}} \circ (f_{r,3} \circ f_{r,2})$. In this internal transition, function $f_{i,2}$ inserts $rCap$ into T_r. Hence, $\sigma' \models |T_r| > 1$. Furthermore, function $f_{i,2}$ returns a valid i-cap, which points to the inserted resource capability inside the tree. Variable $iCap$ keeps the returned intermediate capability. Because $iCap$ points to the inserted $rCap$ inside T_r and $\sigma \models isValidCap(rCap)$, we have $\sigma' \models isValidCap(iCap)$. Function $f_{i,3}$ creates a resource-allocation response for program I_{ra} and assigns it to y_r, such that $isRaRes(y_r) = true$ and $y_r.cap = iCap$. In addition, because $isValidCap(iCap)$, we have $isValidCap(y_r.cap)$. Thus, this verification holds.
- $\models Q_{l_{r,3}} \wedge A^r_{ra} \rightarrow ((A^r_{ra} \rightarrow Q_{l_{r,1}}) \wedge C^r_{ra}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B, \sigma(y_r)))$. In this output transition, program R_{ra} just sends y_r through channel C toward program I_{ra}. C^r_{ra} holds because $\#C = \#D > 0$, $last(D) = \sigma(y_r)$, and $\sigma \models isRaRes(y_r) \wedge isValidCap(y_i.cap)$. Hence, this verification holds.

Since $Q_{t^r_{ra}} \rightarrow \psi^r_{ra}$, the post-condition of program R_{ra} is satisfied.

5.4.3 Resource Allocation - Parallel Composition

This section presents the parallel composition of the resource-allocation components based on the described rule in Section 2.2. Consider the parallel composition $R_{ra} \parallel I_{ra}$. By applying the parallel composition rule, we deduce the following A-C formula:

$$\begin{gathered} \vdash \langle A_{ra},\ C_{ra} \rangle \\ \{\#A = \#B = \#C = \#D = 0 \ \wedge\ |T_r| = |T_i| = 1\} \\ R_{ra} \parallel I_{ra}\ \{false\} \end{gathered}$$

where A_{ra} and C_{ra} are as follows:

$$\begin{aligned} A_{ra} \stackrel{\text{def}}{=}\ & \#A > 0 \rightarrow \\ & isRaReq(last(A)) \ \wedge\ isUniquePID(last(A).spid)) \end{aligned}$$

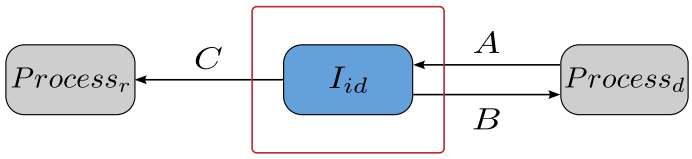


Figure 8: Syntactic Interfaces of the internal-delegation Programs.

$$C_{ra} \stackrel{\text{def}}{=} \#A = \#B = \#C = \#D > 0 \rightarrow \\ (isRaRes(last(B)) \ \wedge \ isValidCap(last(B).cap))$$

Because $\models A_{ra} \ \wedge \ C^i_{ra} \rightarrow A^r_{ra}$ and $\models A_{ra} \ \wedge \ C^r_{ra} \rightarrow A^i_{ra}$. Thus, $R_{ra} \parallel I_{ra}$ generates a valid capability when it receives a resource-allocation request from a process.

□

5.5 Second Lemma: Internal Delegation

The second lemma indicates that the internal delegation of a valid p-cap by a process creates a valid p-cap for another process inside the same node. Hence, the intermediate controller handles the internal delegation inside the node. We formally define the lemma and proof it.

Lemma 2. *Given two processes with unique IDs inside the same process node, delegation of a valid capability from the first process, $process_d$, to the second process, $process_r$, causes $process_r$ and $process_d$ to receive a valid process capability and a valid indicator capability, respectively.*

Proof. We use the assumption-commitment technique to prove the lemma.

We model the intermediate controller in a internal-delegation operation by program $I_{id} \stackrel{\text{def}}{=} (L_{i_id}, T_{i_id}, s_{i_id}, t_{i_id})$ to prove the lemma. Figure 8 depicts the syntactic interfaces between the program and two processes. In addition, figure 9 illustrates sequential diagrams of programs I_{id}. In the next step, we prove that $process_r$ receives a valid p-cap when $process_d$ delegates a valid capability. In addition, we prove that $process_d$ receives a valid p-cap of type indicator to the new capability inside the intermediate-capability tree.

5.5.1 internal Delegation - Intermediate Controller

Program I_{id} receives a internal capability-delegation request from $process_d$ via channel A. The request contains a valid p-cap that points to an intermediate capability inside the intermediate-capability tree. In the next step, program I_{id} delegates the intermediate capability according to the request and inserts the new intermediate capability inside the tree. Finally, program I_{id} creates a delegation response for $procces_r$ and a delegation-confirmation response for $process_d$, respectively. The delegation response

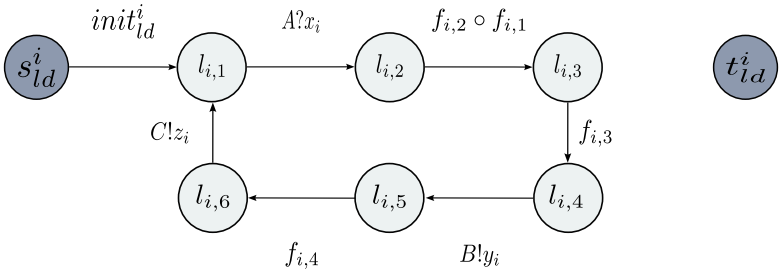


Figure 9: Internal Delegation - Program I_{id}.

and the delegation-confirmation response contain the new p-cap and the new indicator capability, respectively. The functions of I_{id} are as follows:

$$
\begin{aligned}
init^i_{id}(\sigma) &= (\sigma : rootPtr \mapsto getRoot(\sigma(icTree))),\\
f_{i,1}(\sigma) &= (\sigma : indCap \mapsto delegate(\sigma(rootPtr), \sigma(x_i))),\\
f_{i,2}(\sigma) &= (\sigma : pCap \mapsto genCapFromInd(\sigma(icTree), \sigma(indCap))),\\
f_{i,3}(\sigma) &= (\sigma : y_i \mapsto genLdConfRes(\sigma(x_i), \sigma(indCap))),\\
f_{i,4}(\sigma) &= (\sigma : z_i \mapsto genLdRes(\sigma(x_i), \sigma(pCap)))
\end{aligned}
$$

The A-C formula for process I_{id} is as follows:

$$\vdash \langle Ass^i_{id},\ C^i_{id}\rangle\ \{\varphi^i_{id}\}\ I_{id}\ \{\psi^i_{id}\}$$

where the formal definition of φ^i_{id}, ψ^i_{id}, Ass^i_{id}, and C^i_{id} are as follows:

$$
\begin{aligned}
\varphi^i_{id} &\stackrel{\text{def}}{=} \#A = \#B = \#C = 0\ \wedge\ |icTree| > 1\\
\psi^i_{id} &\stackrel{\text{def}}{=} false\\
Ass^i_{id} &\stackrel{\text{def}}{=} \#A > 0 \rightarrow\\
&\quad (isIdReq(last(A))\ \wedge\ isValidCap(last(A).cap) \wedge\\
&\quad isCurrentNode(last(A).snid) \wedge\\
&\quad isCurrentNode(last(A).rnid)) \wedge\\
&\quad isUniquePID(last(A).spid)\ \wedge\ isUniquePID(last(A).rpid)))\\
C^i_{id} &\stackrel{\text{def}}{=} (\#A = \#B > \#C \rightarrow\\
&\quad isDelConfRes(last(B))\ \wedge\ isValidInd(last(B).cap)) \wedge\\
&\quad (\#A = \#B = \#C > 0 \rightarrow\\
&\quad isLdRes(last(C))\ \wedge\ isValidCap(last(C).cap)
\end{aligned}
$$

The assertion network for I_{id} is as follows:

$$Q_{s^i_{id}} \stackrel{\text{def}}{=} \#A = \#B = \#C = 0\ \wedge\ |icTree| > 1$$

$$Q_{l_{i,1}} \stackrel{\text{def}}{=} \#A = \#B = \#C \ \wedge \ |icTree| > 1$$

$$Q_{l_{i,2}} \stackrel{\text{def}}{=} \#B = \#C = (\#A - 1) \ \wedge \ last(A) = x_i \ \wedge \ |icTree| > 1 \ \wedge$$
$$isIdReq(last(A)) \ \wedge \ isValidCap(last(A).cap) \ \wedge$$
$$isCurrentNode(last(A).snid) \ \wedge \ isCurrentNode(last(A).rnid)) \ \wedge$$
$$isUniquePID(last(A).spid) \ \wedge \ isUniquePID(last(A).rpid)))$$

$$Q_{l_{i,3}} \stackrel{\text{def}}{=} \#B = \#C = (\#A - 1) \ \wedge \ last(A) = x_i \ \wedge \ |icTree| > 2 \ \wedge$$
$$isValidInd(iCap)) \ \wedge \ isValidCap(pCap))$$

$$Q_{l_{i,4}} \stackrel{\text{def}}{=} \#B = \#C = (\#A - 1) \ \wedge \ last(A) = x_i \ \wedge \ |icTree| > 2 \ \wedge$$
$$isValidCap(pCap)) \ \wedge \ isDelConfRes(y_i) \ \wedge \ isValidInd(y_i.cap)$$

$$Q_{l_{i,5}} \stackrel{\text{def}}{=} \#A = \#B = (\#C + 1) \ \wedge \ last(A) = x_i \ \wedge \ \ last(B) = y_i \ \wedge$$
$$|icTree| > 2 \ \wedge \ isLdRes(z_i) \ \wedge \ isValidCap(z_i.cap))$$

$$Q_{l_{i,6}} \stackrel{\text{def}}{=} \#A = \#B = (\#C + 1) \ \wedge \ last(A) = x_i \ \wedge \ \ last(B) = y_i \ \wedge$$
$$|icTree| > 2 \ \wedge \ isLdRes(z_i) \ \wedge \ isValidCap(z_i.cap))$$

$$Q_{t^i_{id}} \stackrel{\text{def}}{=} false$$

We check the following implications to prove that the above assertion network is an A-C-inductive assertion network w.r.t. assumption Ass^i_{id}, commitment C^i_{id}, and channels A, B, and C.

- $\models Q_{s^i_{id}} \rightarrow C^i_{id}$ follows from the above definitions.
- $\models Q_{s^i_{id}} \ \wedge \ Ass^i_{id} \ \rightarrow \ Q_{l_{i,1}} \circ init^i_{id}$. In this internal transition, the size of the intermediate-capability tree does not change. Hence, this verification holds.
- $\models Q_{l_{i,1}} \ \wedge \ Ass^i_{id} \ \rightarrow \ ((Ass^i_{id} \ \rightarrow \ Q_{l_{i,2}}) \ \wedge \ C^i_{id}) \circ (f_{i,2} \circ f_{i,1} \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x_i, \ h \mapsto v, \ \sigma(h).(A, v))$ for arbitrary value v. In this input transition, communication through channel A just took place, and function g assigns the received value to x_i. Since $\#A > 0$, the first implication of Ass^i_{id} satisfies that the received message is a internal-delegation request, and both the delegator and the receiver processes have unique PIDs. Thus, this verification holds.
- $\models Q_{l_{i,2}} \ \wedge \ Ass^i_{id} \ \rightarrow \ Q_{l_{i,3}} \circ (f_{i,2} \circ f_{i,1})$. In this internal transition, function $f_{i,1}$ delegates the $x_i.cap$, creates a valid indicator capability pointing to the new i-cap inside the intermediate-capability tree, and assigns it to $indCap$. Hence, we have $\sigma' \models |icTree| > 2$. Furthermore, function $f_{i,2}$ creates a valid p-cap corresponding to $indCap$ and assigns it to $pCap$. Hence, this verification holds.
- $\models Q_{l_{i,3}} \ \wedge \ Ass^i_{id} \ \rightarrow \ Q_{l_{i,4}} \circ f_{i,3}$. In this internal transition, function $f_{i,3}$ creates a delegation-confirmation response for the delegator process and assigns it to y_i, wherein $y_i.cap = indCap$. Hence, y_i contains a valid indicator capability. Thus, this verification holds.
- $\models Q_{l_{i,4}} \ \wedge \ Ass^i_{id} \ \rightarrow \ ((Ass^i_{id} \ \rightarrow \ Q_{l_{i,5}}) \ \wedge \ C^i_{id}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B, \sigma(y_i)))$. In this output transition, program I_{id} sends y_i through channel B.

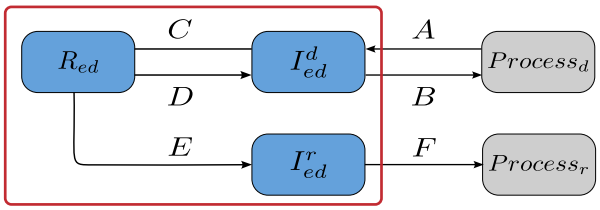


Figure 10: Syntactic Interfaces of the External-delegation Programs.

C^i_{id} holds because $last(B) = \sigma(y_i)$ and $\sigma \models isLdConfRes(y_i) \wedge isValidInd(y_i.cap)$. Hence, this verification holds.

- $\models Q_{l_{i,5}} \wedge Ass^i_{id} \rightarrow Q_{l_{i,6}} \circ f_{i,4}$. In this internal transition, function $f_{i,4}$ creates a delegation response for the receiver process and assigns it to z_i, wherein $z_i.cap = pCap$. Hence, z_i contains a valid process capability. Thus, this verification holds.
- $\models Q_{l_{i,6}} \wedge Ass^i_{id} \rightarrow ((Ass^i_{id} \rightarrow Q_{l_{i,1}}) \wedge C^i_{id}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(C, \sigma(z_i)))$. In this output transition, program I_{id} sends z_i through channel C. C^i_{id} holds because $\sigma \models isLdRes(z_i) \wedge isValidCap(z_i.cap)$. Hence, this verification holds.

Since $Q_{t^i_{id}} \rightarrow \psi^i_{id}$, the post-condition of program I_{id} is satisfied.

□

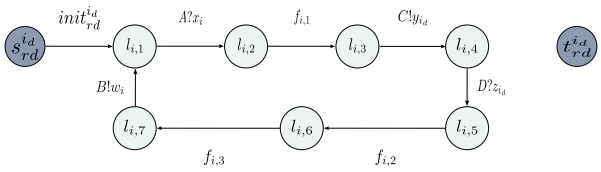
5.6 Third Lemma: External Delegation

The Third lemma indicates that delegating a valid p-cap by the delegator process creates a valid p-cap for a process inside another node. This operation requires that both intermediate controllers and the resource controller participate. We formally define the lemma and proof it.

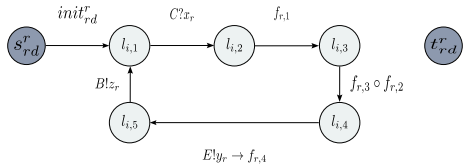
Lemma 3. *Given two processes with unique PIDs inside different process nodes, delegating a valid capability from the first process to the second process causes that the receiver and the delegator processes receive a valid p-cap and a valid indicator, respectively.*

Proof. We use the assumption-commitment technique to prove the lemma.

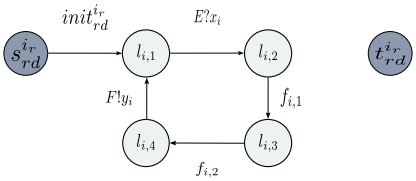
To proof the lemma, we model the intermediate controller, operating at the delegator-process side, the resource controller, and the intermediate controller, operating at the receiver-process side, in a external-delegation operation by programs $I^d_{ed} \stackrel{\text{def}}{=} (L^{i_d}_{ed}, T^{i_d}_{ed}, s^{i_d}_{ed}, t^{i_d}_{ed})$, $R_{ed} \stackrel{\text{def}}{=} (L^r_{ed}, T^r_{ed}, s^r_{ed}, t^r_{ed})$, and $I^r_{ed} \stackrel{\text{def}}{=} (L^{i_r}_{ed}, T^{i_r}_{ed}, s^{i_r}_{ed}, t^{i_r}_{ed})$, respectively. Figure 10 depicts these three programs and their syntactic interfaces. The messages are exchanged between the programs via the channels to handle external-delegation requests. In addition, figures 11a, 11b, and 11c illustrate sequential diagrams of programs I^d_{ed}, R_{ed}, and I^r_{ed}, respectively. In the next step, we prove that the receiver process will receive a valid p-cap. In addition, we prove that process the delegator process receives a valid indicator capability.



(a) Program I^d_{ed}.



(b) Program R_{ed}.



(c) Program I^r_{ed}.

Figure 11: external-Delegation Processes.

5.6.1 External Delegation - Delegating-Side Intermediate Controller

Program I^d_{ed} receives a external-delegation request from the process via channel A, creates a corresponding request for program R_{ed}, and sends it through channel C. Furthermore, It receives the response from program R_{ed} via channel D. Program I^d_{ed} updates its capability tree when it receives an i-cap from the resource controller by inserting the indicator capability inside its tree. In addition, it creates the corresponding indicator capability for the inserted capability inside its tree. Finally, program I^d_{ed} creates a response for the process and sends the indicator inside the response to the process through channel B. The conditions and functions of I^d_{ed} are as follow:

$$
\begin{aligned}
init^{i_d}_{ed}(\sigma) &= (\sigma : rootPtr \mapsto getRoot(\sigma(icTree))),\\
f_{i,1}(\sigma) &= (\sigma : y_i \mapsto genRdReq(\sigma(rootPtr), \sigma(x_i)),\\
f_{i,2}(\sigma) &= (\sigma : pIndCap \mapsto insert(\sigma(icTree), \sigma(z_i))),\\
f_{i_d,3}(\sigma) &= (\sigma : w_i \mapsto genRdConfRes(\sigma(x), \sigma(pIndCap)))
\end{aligned}
$$

The A-C formula for process I^d_{ed} is as follows:

$$\vdash \langle Ass^{i_d}_{ed},\ C^{i_d}_{ed} \rangle\ \{\varphi^{i_d}_{ed}\}\ I^d_{ed}\ \{\psi^{i_d}_{ed}\}$$

where the formal definition of $\varphi_{ed}^{i_d}$, $\psi_{ed}^{i_d}$, $Ass_{ed}^{i_d}$, and $C_{ed}^{i_d}$ are as follows:

$$\varphi_{ed}^{i_d} \stackrel{\text{def}}{=} \#A = \#B = \#C = \#D = 0 \ \wedge \ |icTree| > 1$$

$$\psi_{ed}^{i_d} \stackrel{\text{def}}{=} false$$

$$\begin{aligned} Ass_{ed}^{i_d} \stackrel{\text{def}}{=} \ & (\#A > 0 \rightarrow \\ & (isRdReq(last(A)) \ \wedge \ isValidCap(last(A).cap) \wedge \\ & isUniquePID(last(A).spid) \wedge \\ & isUniquePID(last(A.rpid))) \wedge \\ & (\#C = \#D > 0 \rightarrow \\ & \quad isEdConfRes(last(D)) \ \wedge \ isValidInd(last(D).cap))) \wedge \end{aligned}$$

$$\begin{aligned} C_{ed}^{i_d} \stackrel{\text{def}}{=} \ & (\#A = \#B > 0 \rightarrow \\ & \quad isEdConfRes(last(B)) \ \wedge \ isValidInd(last(B).cap)) \wedge \\ & (\#C > 0 \rightarrow (isRdReq(last(C)) \ \wedge \ isValidCap(last(C).cap) \wedge \\ & \ isUniquePID(last(C).spid) \ \wedge \ isUniquePID(last(C).rpid))) \end{aligned}$$

The assertion network for I_{ed}^{d} is as follows:

$$Q_{s_{ed}^{i_d}} \stackrel{\text{def}}{=} \#A = \#B = \#C = \#D = 0 \ \wedge \ |icTree| > 1$$

$$Q_{l_{i,1}} \stackrel{\text{def}}{=} \#A = \#B = \#C = \#D$$

$$\begin{aligned} Q_{l_{i,2}} \stackrel{\text{def}}{=} \ & \#B = \#C = \#D = (\#A - 1) \ \wedge \ last(A) = x_i \wedge \\ & isRdReq(last(A)) \ \wedge \ isValidCap(last(A).cap)) \wedge \\ & isUniquePID(last(A).spid) \ \wedge \ isUniquePID(last(A).rpid) \end{aligned}$$

$$\begin{aligned} Q_{l_{i,3}} \stackrel{\text{def}}{=} \ & \#B = \#C = \#D = (\#A - 1) \ \wedge \ last(A) = x_i \wedge \\ & isRdReq(y_i) \ \wedge \ isValidInd(y_i.cap)) \ \wedge \ isUniquePID(y_i.spid) \wedge \\ & isUniquePID(y_i.rpid) \end{aligned}$$

$$Q_{l_{i,4}} \stackrel{\text{def}}{=} \#A = \#B = (\#A - 1) = (\#C - 1) \ \wedge \ last(A) = x_i \ \wedge \ last(C) = y_i$$

$$\begin{aligned} Q_{l_{i,5}} \stackrel{\text{def}}{=} \ & \#A = \#C = \#D = (\#B + 1) \ \wedge \ last(A) = x_i \ \wedge \ last(C) = y_i \wedge \\ & last(D) = z_i \ \wedge \ isEdConfRes(last(D)) \ \wedge \ isValidInd(last(D).cap) \end{aligned}$$

$$\begin{aligned} Q_{l_{i,6}} \stackrel{\text{def}}{=} \ & \#A = \#C = \#D = (\#B + 1) \ \wedge \ last(A) = x_i \ \wedge \ last(C) = y_i \wedge \\ & last(D) = z_i \ \wedge \ isValidInd(pIndCap) \end{aligned}$$

$$\begin{aligned} Q_{l_{i,7}} \stackrel{\text{def}}{=} \ & \#A = \#C = \#D = (\#B + 1) \ \wedge \ last(A) = x_i \ \wedge \ last(C) = y_i \wedge \\ & last(D) = z_i \ \wedge \ isEdConfRes(w_i) \ \wedge \ isValidInd(w_i.cap) \end{aligned}$$

$$Q_{t_{ed}^{i_d}} \stackrel{\text{def}}{=} false$$

We check the following implications to prove that the above assertion network is an A-C-inductive assertion network w.r.t. assumption $Ass^{i_d}_{ed}$, commitment $C^{i_d}_{ed}$, and channels A, B, C, and D.

- $\models Q_{s^{i_d}_{ed}} \rightarrow C^{i_d}_{ed}$ follows from the above definitions.
- $\models Q_{s^{i_d}_{ed}} \wedge Ass^{i_d}_{ed} \rightarrow Q_{l_{i,1}} \circ init^{i_d}_{ed}$. In this internal transition, just function $init^{i^d}_{ed}$ gets a pointer to the root of the capability tree. Hence, this verification holds.
- $\models Q_{l_{i,1}} \wedge Ass^{i_d}_{ed} \rightarrow ((Ass^{i_d}_{ed} \rightarrow Q_{l_{i,2}}) \wedge C^{i_d}_{ed}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x_i,\ h \mapsto v,\ \sigma(h).(A, v))$ for arbitrary value v. In this input transition, just communication through channel A took place, and function g assigns the received value to x_i. Because $\#A > 0$, the first implication of $Ass^{i_d}_{ed}$ satisfies that it is a external-delegation request, $last(A).cap$ is a valid indicator capability, and the delegator and receiver PIDs are unique. Thus, this verification holds.
- $\models Q_{l_{i,2}} \wedge Ass^{i_d}_{ed} \rightarrow Q_{l_{i,3}} \circ f_{i,1}$. In this internal transition, function $f_{i,1}$ creates a external-revocation request and assigns it to variable y_i, such that $isRdReq(y_i) = true$, $y_i.spid = last(A).spid$, and $y_i.rpid = last(A).rpid$. Hence, the delegator and receiver PIDs in the new request are unique because Ass^{i}_{ra} indicates that both PIDs inside the request from the process are unique. Thus, this verification holds.
- $\models Q_{l_{i,3}} \wedge Ass^{i_d}_{ed} \rightarrow ((Ass^{i_d}_{ed} \rightarrow Q_{l_{i,7}}) \wedge C^{i_d}_{ed}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(C, \sigma(y_i)))$. In this output transition, program I^d_{ed} sends y_i through channel C. $C^{i_d}_{ed}$ holds because $last(C) = \sigma(y_i)$, $isRdReq(y_i)$, and both $y_i.spid$ and $y_i.rpid$ are unique. Hence, this verification holds.
- $\models Q_{l_{i,4}} \wedge Ass^{i_d}_{ed} \rightarrow ((Ass^{i_d}_{ed} \rightarrow Q_{l_{i,5}}) \wedge C^{i_d}_{ed}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : z_i,\ h \mapsto v,\ \sigma(h).(D, v))$ for arbitrary value v. In this input transition, a communication through channel D took place, and function g assigns the received value to z_i. Because $\#D > 0$, $Ass^{i_d}_{ed}$ implies that $isEdConfRes(last(D))$ and $isValidInd(last(D).cap)$. Thus, this verification holds.
- $\models Q_{l_{i,5}} \wedge Ass^{i_d}_{ed} \rightarrow Q_{l_{i,6}} \circ f_{i,2}$. In this internal transition, function $f_{i,2}$ inserts the received intermediate indicator into the capability tree and returns $pIndCap$ that points to it inside the tree. We have $isValidCap(pIndCap)$ because $ValidInd(last(D).cap)$, and $pIndCap$ points to the it after the intermediate controller inserts it inside the tree. Thus, this verification holds.
- $\models Q_{l_{i,6}} \wedge Ass^{i_d}_{ed} \rightarrow Q_{l_{i,7}} \circ (f_{i,3} \circ f_{i,2})$. In this internal transition, function $f_{i,3}$ creates a external-delegation confirmation response for the process and assigns it to w_i, wherein $w_i.cap = pIndCap$. Thus, this verification holds.
- $\models Q_{l_{i,7}} \wedge Ass^{i_d}_{ed} \rightarrow ((Ass^{i_d}_{ed} \rightarrow Q_{l_{i,1}}) \wedge C^{i_d}_{ed}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B, \sigma(w_i)))$. In this output transition, program I^d_{ed} sends w_i through channel B. $C^{i_d}_{ed}$ holds because $\sigma \models isEdConfRes(w_i) \wedge isValidInd(w_i.cap)$. Hence, this verification holds.

Because $Q_{t^{i_d}_{ed}} \rightarrow \psi^{i_d}_{ed}$, the post-condition of program I^d_{ed} is satisfied.

5.6.2 External Delegation - Resource Controller

Program R_{ed} receives a external-delegation request from program I^d_{ed} via channel C. In the next step, program R_{ed} creates creates the delegated capability and inserts it inside the capability tree. Furthermore, it creates the delegated resource capability's corresponding intermediate and indicator capabilities. Afterward, program R_{ed} creates the external-delegation and confirmation responses and inserts the intermediate and indicator capabilities inside them. Finally, it sends the responses through channels E and D toward programs I^r_{ed} and I^d_{ed}, respectively. The functions of R_{ed} are as follows:

$$
\begin{aligned}
init^r_{ed}(\sigma) &= (\sigma : rootPtr \mapsto getRoot(\sigma(rcTree))),\\
f_{r,1}(\sigma) &= (\sigma : indCap \mapsto delegate(\sigma(rootPtr), \sigma(x_r))),\\
f_{r,2}(\sigma) &= (\sigma : iCap \mapsto genCapFromInd(\sigma(indCap), \sigma(indCap))),\\
f_{r,3}(\sigma) &= (\sigma : y_r \mapsto genRdRes(\sigma(x_r), \sigma(iCap))),\\
f_{r,3}(\sigma) &= (\sigma : z_r \mapsto genRdConfRes(\sigma(x_r), \sigma(indCap))),
\end{aligned}
$$

where $rcTree$ is the resource-capability tree, $indCap$ is an intermediate indicator, and $iCap$ is an intermediate capability.

The A-C formula for process R_{ed} is as follows:

$$\vdash \langle Ass^r_{ed}\ C^r_{ed}\rangle\ \{\varphi^r_{ed}\}\ R_{ed}\ \{\psi^r_{ed}\}$$

where the formal definition of φ_r, ψ_r , Ass_r, and C_r are as follows:

$$
\begin{aligned}
\varphi^r_{ed} &\stackrel{\text{def}}{=} \#C = \#D = \#E = 0\ \wedge\ |rcTree| \geqslant 1\\
\psi^r_{ed} &\stackrel{\text{def}}{=} false\\
Ass^r_{ed} &\stackrel{\text{def}}{=} (\#C > 0 \rightarrow\\
&\quad (isRdReq(last(C))\ \wedge\ isValidInd(last(C).cap)\ \wedge\\
&\quad\ isUniquePID(last(C).spid)\ \wedge\\
&\quad\ isUniquePID(last(C).rpid)))\\
C^r_{ed} &\stackrel{\text{def}}{=} (\#C = \#D > 0 \rightarrow\\
&\quad (isEdConfRes(last(D))\ \wedge\ isValidInd(last(D).cap)))\ \wedge\\
&\quad (\#C = \#E > 0 \rightarrow\\
&\quad (isRdRes(last(E))\ \wedge\ isValidCap(last(E).cap)))
\end{aligned}
$$

The assertion network for R_{ed} is as follows:

$$
\begin{aligned}
Q_{s^r_{ed}} &\stackrel{\text{def}}{=} \#C = \#D = \#E = 0\ \wedge\ |rcTree| \geqslant 1\\
Q_{r_1} &\stackrel{\text{def}}{=} \#C = \#D = \#E\\
Q_{r_2} &\stackrel{\text{def}}{=} \#D = \#E = (\#C - 1)\ \wedge\ last(C) = x_r\ \wedge\ isRdReq(last(C))\ \wedge\\
&\quad isValidInd(last(C).cap)\ \wedge\ isUniquePID(last(C).spid)\ \wedge
\end{aligned}
$$

$$isUniquePID(last(C).rpid)$$

$$Q_{r_3} \stackrel{\text{def}}{=} \#D = \#E = (\#C - 1) \ \wedge \ last(C) = x_r \ \wedge \ isValidInd(indCap)$$

$$Q_{r_4} \stackrel{\text{def}}{=} \#D = \#E = (\#C - 1) \ \wedge \ last(C) = x_r \ \wedge \ isValidInd(indCap) \wedge isRdRes(y_r) \ \wedge \ isValidCap(y_r.cap)$$

$$Q_{r_5} \stackrel{\text{def}}{=} \#C = \#E = (\#D + 1) \ \wedge \ last(C) = x_r \ \wedge \ last(E) = y_r \wedge isEdConfRes(z_r) \ \wedge \ isValidInd(z_r.cap)$$

$$Q_{t^r_{ed}} \stackrel{\text{def}}{=} false$$

We check the following implications to prove that the above assertion network is an A-C-inductive assertion network w.r.t. assumption Ass^r_{ed}, commitment C^r_{ed}, and channels C, D, and E.

- $\models Q_{s^r_{ed}} \rightarrow C^r_{ed}$ follows from the above definitions.
- $\models Q_{s^r_{ed}} \wedge Ass^r_{ed} \rightarrow Q_{l_{r,1}} \circ init^r_{ed}$. In this internal transition, just function $init^r_{ed}$ gets a pointer to the root of the capability tree. Hence, this verification holds.
- $\models Q_{l_{r,1}} \ \wedge \ Ass^r_{ed} \rightarrow ((Ass^r_{ed} \rightarrow Q_{r_2}) \ \wedge \ C^r_{ed}) \circ$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x_r, \ h \mapsto v, \ \sigma(h).(C, v))$ for arbitrary v. In this input transition, a communication through channel C just took place. Function g assigns the last received value from channel C to x_r. Because $\#C > 0$, the first implication of Ass^r_{ed} satisfies that the request is a resource allocation one, the process IDs of the delagator and receiver processes are unique, delegator, and the request contains a valid indicator. C^r_{ed} holds because neither $\#C = \#D$ nor $\#C = \#E$. Thus, this verification holds.
- $\models Q_{l_{r,2}} \ \wedge \ Ass^r_{ed} \rightarrow Q_{l_{r,3}} \circ (unlockTree \circ f_{r,1})$. In this internal transition, function $f_{r,1}$ delegates the capability and inserts the newly generated capability into the capability tree. Furthermore, function $f_{r,1}$ returns a valid indicator capability that points to the inserted resource capability inside the tree. Variable $indCap$ keeps the returned intermediate indicator. Hence, we have $\sigma' \models isValidInd(indCap)$. Thus, this verification holds.
- $\models Q_{l_{r,3}} \wedge Ass^r_{ed} \rightarrow Q_{l_{r,4}} \circ (f_{r,3} \circ f_{r,2})$. In this internal transition, function $f_{r,2}$ generates a intermediate capability from the newly generated resource capability and assign it to variable $iCap$. Hence, we have $isValidCap(iCap)$. Afterward, function $f_{r,3}$ creates external-delegation response and inserts $iCap$ as its capability. Thus, this verification holds.
- $\models Q_{l_{r,4}} \ \wedge \ Ass^r_{ed} \rightarrow ((Ass^r_{ed} \rightarrow Q_{l_{r,5}}) \ \wedge \ C^r_{ed}) \circ (f_{r,3} \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(E, \sigma(y_r)))$. In this output transition, program R_{ed} sends y_r through channel E. Commitment C^r_{ed} holds because we have $isRdRes(y_r)$ and $isValidCap(y_r.cap)$. Afterward, function $f_{r,3}$ creates a external-delegation confirmation response, inserts $indCap$ as its capability, and assigns it to variable z_r. Hence, it satisfies both $isEdConfRes(z_r)$ and $isValidInd(z_r.cap)$. Thus, this verification holds.
- $\models Q_{l_{r,5}} \ \wedge \ Ass^r_{ed} \rightarrow ((Ass^r_{ed} \rightarrow Q_{l_{r,1}}) \ \wedge \ C^r_{ed}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B, \sigma(y_r)))$. In this output transition, program R_{ed} sends z_r through chan-

nel B. Commitment C^r_{ed} holds because Z_r is a external-delegation-confirmation response and contains a valid indicator. Thus, this verification holds.

Because $Q_{t^r_{ed}} \rightarrow \psi^r_{ed}$, the post-condition of program R_{ed} is satisfied.

5.6.3 External Delegation - Receiving-Side Intermediate Controller

Program I^r_{ed} receives a external-delegation request from the process via channel E. Then, it updates its capability tree by inserting the received intermediate capability inside the tree. In addition, it creates the corresponding p-cap for the inserted i-cap. Finally, program I^r_{ed} creates a external-delegation response for the receiving process and sends the p-cap inside the response to the process through channel B. The functions of I^r_{ed} are as follows:

$$\begin{aligned} init^{i_r}_{ed}(\sigma) &= (\sigma : rootPtr \mapsto getRoot(\sigma(icTree))), \\ f_{i,1}(\sigma) &= (\sigma : pCap \mapsto insert(\sigma(rootPtr), \sigma(x_i.cap))) \\ f_{i,2}(\sigma) &= (\sigma : y_i \mapsto genRdRes(\sigma(x_i), \sigma(pCap))), \end{aligned}$$

The A-C formula for process I^d_{ed} is as follows:

$$\vdash \langle Ass^{i_r}_{ed},\ C^{i_r}_{ed} \rangle\ \{\varphi^{i_r}_{ed}\}\ I^r_{ed}\ \{\psi^{i_r}_{ed}\}$$

where the formal definition of $\varphi^{i_r}_{ed}$, $\psi^{i_r}_{ed}$, $Ass^{i_r}_{ed}$, and $C^{i_r}_{ed}$ are as follows:

$$\begin{aligned} \varphi^{i_r}_{ed} &\stackrel{\text{def}}{=} \#E = \#F = 0\ \wedge\ |icTree| \geqslant 1 \\ \psi^{i_r}_{ed} &\stackrel{\text{def}}{=} false \\ Ass^{i_r}_{ed} &\stackrel{\text{def}}{=} \#E > 0 \rightarrow \\ &\quad (isRdRes(last(E))\ \wedge\ isValidCap(last(E).cap) \\ C^{i_r}_{ed} &\stackrel{\text{def}}{=} \#E = \#F > 0 \rightarrow \\ &\quad isRdRes(last(F))\ \wedge\ isValidCap(last(F).cap) \end{aligned}$$

The assertion network for I^r_{ed} is as follows:

$$\begin{aligned} Q_{s^{i_r}_{ed}} &\stackrel{\text{def}}{=} \#E = \#F = 0\ \wedge\ |icTree| \geqslant 1 \\ Q_{l_{i,1}} &\stackrel{\text{def}}{=} \#E = \#F \\ Q_{l_{i,2}} &\stackrel{\text{def}}{=} \#F = (\#E - 1)\ \wedge\ last(E) = x_i\ \wedge \\ &\quad isRdRes(last(E))\ \wedge\ isValidCap(last(E).cap)) \\ Q_{l_{i,3}} &\stackrel{\text{def}}{=} \#F = (\#E - 1)\ \wedge\ last(E) = x_i\ \wedge \\ &\quad isValidCap(pCap) \\ Q_{l_{i,4}} &\stackrel{\text{def}}{=} \#F = (\#E - 1)\ \wedge\ last(E) = x_i\ \wedge \end{aligned}$$

$$isRdRes(y_i) \ \wedge \ isValidCap(y_i.cap))$$

$$Q_{t^{i_d}_{ed}} \stackrel{\text{def}}{=} false$$

We check the following implications to prove that the above assertion network is an A-C-inductive assertion network w.r.t. assumption $Ass^{i_r}_{ed}$, commitment $C^{i_r}_{ed}$, and channels E and F.

- $\models Q_{s^{i_r}_{ed}} \rightarrow C^{i_r}_{ed}$ follows from the above definitions.
- $\models Q_{s^{i^r}_{ed}} \wedge Ass^{i_r}_{ed} \rightarrow Q_{l_{i,1}} \circ init^{i^r}_{ed}$. In this internal transition, just function $init^{i^r}_{ed}$ gets a pointer to the root of the capability tree. Hence, this verification holds.
- $\models Q_{l_{i,1}} \ \wedge \ Ass^{i_r}_{ed} \rightarrow ((Ass^{i_r}_{ed} \rightarrow Q_{l_{i,2}}) \ \wedge \ C^{i_r}_{ed}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x_i, \ h \mapsto v, \ \sigma(h).(A, v))$ for arbitrary value v. In this input transition, just communication through channel A took place, and function g assigns the received value to x_i. Because $\#A > 0$, the first implication of $Ass^{i_r}_{ed}$ satisfies that the last received message is a external-delegation response,and the capability inside it is a valid intermediate capability. Thus, this verification holds.
- $\models Q_{l_{i,2}} \ \wedge \ Ass^{i_r}_{ed} rightarrow Q_{l_{i,3}} \circ f_{i,1}$. In this internal transition, function $f_{i,1}$ inserts the received intermediate capability into the capability tree and returns $pCap$ that points to it inside the tree. Hence, we have $isValidCap(pCap)$. Thus, this verification holds.
- $\models Q_{l_{i,3}} \wedge Ass^{i_r}_{ed} \rightarrow Q_{l_{i,4}} \circ (f_{i,2} \circ unlockTree)$. In this internal transition, function $f_{i,2}$ creates a external-delegation response for the process and assigns it to y_i, wherein $y_i.cap = pCap$. Hence, this verification holds.
- $\models Q_{l_{i,4}} \ \wedge \ Ass^{i_r}_{ed} \rightarrow ((Ass^{i_r}_{ed} \rightarrow Q_{l_{i,1}}) \ \wedge \ C^{i_r}_{ed}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(F, \sigma(y_i)))$. In this output transition, program I^r_{ed} sends y_i through channel F. $C^{i_r}_{ed}$ holds because $\sigma \models isRdRes(y_i) \wedge isValidCap(y_i.cap)$. Thus, this verification holds.

Because $Q_{t^{i_r}_{ed}} \rightarrow \psi^{i_r}_{ed}$, the post-condition of program I^r_{ed} is satisfied.

5.6.4 External Delegation - Parallel Composition

This section presents the parallel composition of the external-delegation components based on the described rule in 1. Consider the parallel composition $R_{ed} \parallel I^d_{ed} \parallel I^r_{ed}$. Program R_{ed} satisfies the assumption-commitment pair $(Ass^r_{ed}, \ C^r_{ed})$ as follows:

$$\vdash \langle Ass^r_{ed} \ C^r_{ed} \rangle \ \{\varphi^r_{ed}\} \ R_{ed} \ \{\psi^r_{ed}\}$$

where the formal definition of φ_r, ψ_r , Ass_r, and C_r are as follows:

$$\varphi^r_{ed} \quad \stackrel{\text{def}}{=} \quad \#C = \#D = \#E = 0 \ \wedge \ |rcTree| \geqslant 1$$

$$\psi^r_{ed} \quad \stackrel{\text{def}}{=} \quad false$$

$$
\begin{array}{lcl}
Ass^{r}_{ed} & \stackrel{\text{def}}{=} & (\#C > 0 \rightarrow \\
 & & \quad (isRdReq(last(C)) \ \wedge \ isValidInd(last(C).cap) \wedge \\
 & & \quad isUniquePID(last(C).spid) \wedge \\
 & & \quad isUniquePID(last(C).rpid))) \\
C^{r}_{ed} & \stackrel{\text{def}}{=} & (\#C = \#D > 0 \rightarrow \\
 & & \quad (isEdConfRes(last(D)) \ \wedge \ isValidInd(last(D).cap))) \wedge \\
 & & (\#C = \#E > 0 \rightarrow \\
 & & \quad (isRdRes(last(E)) \ \wedge \ isValidCap(last(E).cap)))
\end{array}
$$

Program I^{d}_{ed} satisfies the assumption-commitment pair $(Ass^{i_d}_{ed},\ C^{i_d}_{ed})$ as follows:

$$\vdash \langle Ass^{i_d}_{ed},\ C^{i_d}_{ed} \rangle \ \{\varphi^{i_d}_{ed}\}\ I^{d}_{ed}\ \{\psi^{i_d}_{ed}\}$$

where the formal definition of $\varphi^{i_d}_{ed}$, $\psi^{i_d}_{ed}$, $Ass^{i_d}_{ed}$, and $C^{i_d}_{ed}$ are as follows:

$$
\begin{array}{lcl}
\varphi^{i_d}_{ed} & \stackrel{\text{def}}{=} & \#A = \#B = \#C = \#D = 0 \ \wedge \ |icTree_d| > 1 \\
\psi^{i_d}_{ed} & \stackrel{\text{def}}{=} & false \\
Ass^{i_d}_{ed} & \stackrel{\text{def}}{=} & (\#A > 0 \rightarrow \\
 & & \quad (isRdReq(last(A)) \ \wedge \ isValidCap(last(A).cap) \wedge \\
 & & \quad isUniquePID(last(A).spid) \wedge \\
 & & \quad isUniquePID(last(A.rpid))) \wedge \\
 & & (\#C = \#D > 0 \rightarrow \\
 & & \quad isEdConfRes(last(D)) \ \wedge \ isValidInd(last(D).cap))) \wedge \\
C^{i_d}_{ed} & \stackrel{\text{def}}{=} & (\#A = \#B > 0 \rightarrow \\
 & & \quad isEdConfRes(last(B)) \ \wedge \ isValidInd(last(B).cap)) \wedge \\
 & & (\#C > 0 \rightarrow \\
 & & \quad (isRdReq(last(C)) \ \wedge \ isValidCap(last(C).cap) \wedge \\
 & & \quad isUniquePID(last(C).spid) \ \wedge \ isUniquePID(last(C).rpid)))
\end{array}
$$

Program I^{r}_{ed} satisfies the assumption-commitment pair $(Ass^{i_r}_{ed},\ C^{i_r}_{ed})$ as follows:

$$\vdash \langle Ass^{i_r}_{ed},\ C^{i_r}_{ed} \rangle \ \{\varphi^{i_r}_{ed}\}\ I^{r}_{ed}\ \{\psi^{i_r}_{ed}\}$$

where the formal definition of $\varphi^{i_r}_{ed}$, $\psi^{i_r}_{ed}$, $Ass^{i_r}_{ed}$, and $C^{i_r}_{ed}$ are as follows:

$$
\begin{array}{lcl}
\varphi^{i_r}_{ed} & \stackrel{\text{def}}{=} & \#E = \#F = 0 \ \wedge \ |icTree_r| \geqslant 1 \\
\psi^{i_r}_{ed} & \stackrel{\text{def}}{=} & false \\
Ass^{i_r}_{ed} & \stackrel{\text{def}}{=} & \#E > 0 \rightarrow \\
 & & \quad (isRdRes(last(E)) \ \wedge \ isValidCap(last(E).cap)
\end{array}
$$

$$C_{ed}^{i_r} \quad \stackrel{\text{def}}{=} \quad \#E = \#F > 0 \rightarrow isRdRes(last(F)) \ \wedge \ isValidCap(last(F).cap)$$

By applying the parallel composition rule, we deduce as follows:

$$\frac{\vdash \langle Ass_{ed},\ C_{ed} \rangle}{\{\varphi_{ed}\}\ R_{ra} \parallel I_{ed}^{d} \parallel I_{ed}^{r}\ \{\psi_{ed}\}}$$

where the formal definition of φ_{ed}, ψ_{ed}, Ass_{ed}, and C_{ed} are as follows:

$$\varphi_{ed} \quad \stackrel{\text{def}}{=} \quad \#A = \#B = \#C = \#D = \#E = \#F = 0 \ \wedge \ |rcTree| \geqslant 1 \wedge |icTree_d| \geqslant 1 \ \wedge \ |icTree_r| \geqslant 1$$

$$\psi_{ed} \quad \stackrel{\text{def}}{=} \quad false$$

$$Ass_{ed} \quad \stackrel{\text{def}}{=} \quad \#A > 0 \rightarrow (isRdReq(last(A)) \ \wedge \ isValidCap(last(A).cap) \wedge isUniquePID(last(A).spid) \wedge isUniquePID(last(A).rpid))$$

$$C_{ed} \quad \stackrel{\text{def}}{=} \quad \#A = \#B = \#C = \#D = \#E = \#F > 0 \rightarrow (isEdConfRes(last(B)) \ \wedge \ isValidInd(last(B).cap) (isRdRes(last(F)) \ \wedge \ isValidCap(last(F).cap))$$

□

5.7 Fourth Lemma: External Revocation

The fourth lemma is about the external-revocation operation. We first describe the external revocation instead of the internal revocation because a process may re-delegate a internally delegated capability to a external process. Hence, a internal-revocation operation may implicitly include several external-revocation operations. The fourth lemma indicates that the external revocation of a valid p-cap by the delegator process will invalidate the delegated p-cap owned by another process inside another node. Since it is a external-revocation operation, the intermediate controller in the delegator-process side and the resource controller handle the revocation together We formally define the lemma and proof it.

Lemma 4. *Given a process with a unique PID in a process node, an intermediate controller in the same node, and a resource controller in a resource node, revoking a delegated p-cap, which points to a resource inside the resource node, to another process inside another node invalidates the delegated p-cap.*

Proof. We use the assumption-commitment technique to prove the lemma.

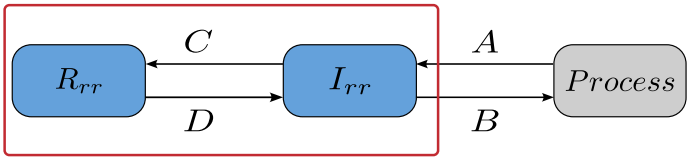


Figure 12: Syntactic Interfaces of the external-revocation Programs.

We model the intermediate controller at the delegator-process side and the resource controller in a external-revocation operation by programs $I_{er} \stackrel{\text{def}}{=} (L^i_{er}, T^i_{er}, s^i_{er}, t^i_{er})$ and $R_{er} \stackrel{\text{def}}{=} (L^r_{er}, T^r_{er}, s^r_{er}, t^r_{er})$, respectively. The programs and the process exchange messages via synchronous channels to handle external-revocation requests. Figure 12 depicts these two programs and their syntactic interfaces. Furthermore, figures 13a and 13b illustrate sequential diagrams of programs I_{er} and R_{er}, respectively. In the next step, we prove that when the process sends a external-revocation request, programs I_{er} and R_{er} revoke the delegated capability and all its re-delegated capabilities.

We need to define a loop-invariant for program I_{er} and a loop-invariant for program R_{er} to prove the correctness of the lemma. When an intermediate controller conducts a external-delegation operation, it inserts an indicator capability as the child of the delegated capability inside its capability tree. There would be no sub-tree after the inserted capability inside the tree because of its indicator type. On the other hand, the resource controller inserts a r-cap inside its capability tree. Hence, the capability may have a sub-tree because of the re-delegation(s).

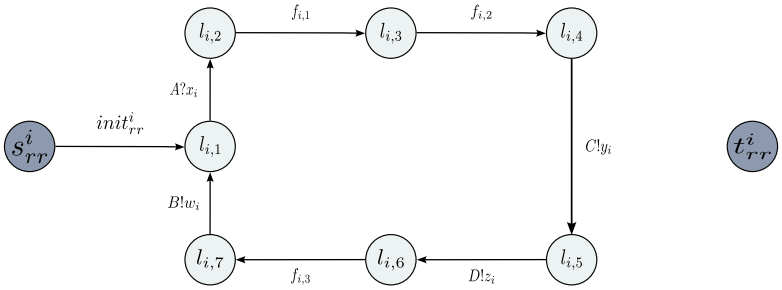
5.7.1 External Revocation - Intermediate Controller

Program I_{er} receives a external-revocation request from the process via channel A. The request contains a valid process indicator that points to an intermediate indicator inside the intermediate-capability tree. In the next step, program I_{er} copies the intermediate indicator and removes it from the tree afterward. Furthermore, it creates a corresponding external-revocation request and sends it through channel C to program R_{er}. Finally, when program I_{er} receives the response from program R_{er} via channel D, it creates a response for the process and sends the response toward the process through channel B. The functions of I_{er} are as follow:

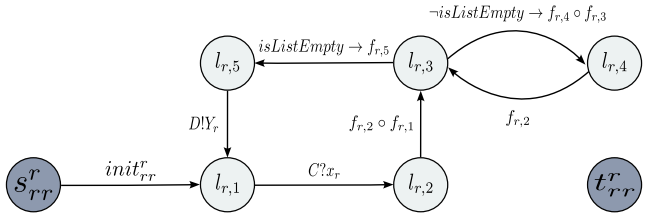
$$
\begin{aligned}
init^i_{er}(\sigma) &= (\sigma : rootPtr \mapsto getRoot(\sigma(icTree))),\\
f_{i,1}(\sigma) &= (\sigma : iIndCap \mapsto revoke(\sigma(rootPtr), \sigma(x_i.cap))),\\
f_{i,2}(\sigma) &= (\sigma : y_i \mapsto genRrReq(\sigma(x_i), \sigma(iIndCap))),\\
f_{i,3}(\sigma) &= (\sigma : w_i \mapsto genRevConfRes(\sigma(z_i)))
\end{aligned}
$$

The A-C formula for program I_{er} is as follows:

$$\vdash \langle Ass^i_{er},\ C^i_{er} \rangle\ \{\varphi^i_{er}\}\ I_{er}\ \{\psi^i_{er}\}$$



(a) Program I_{er}.



(b) Program R_{er}.

Figure 13: external Revocation Programs.

where the formal definition of φ^i_{er}, ψ^i_{er}, Ass^i_{er}, and C^i_{er} are as follows:

$$
\begin{array}{lll}
\varphi^i_{er} & \stackrel{\text{def}}{=} & \#A = \#B = \#C = \#D = 0 \ \wedge \ |icTree| \geqslant 1 \\
\psi^i_{er} & \stackrel{\text{def}}{=} & false \\
Ass^i_{er} & \stackrel{\text{def}}{=} & (\#A > 0 \to \\
 & & \quad isRrReq(last(A)) \ \wedge \ isUniquePID(last(A).spid))) \\
 & & \quad isValidInd(last(A).cap)) \wedge \\
 & & (\#C = \#D > 0 \to isRrConfRes(last(D))) \\
C^i_{er} & \stackrel{\text{def}}{=} & (\#A = \#B = \#C = \#D > 0 \to isRrConfRes(last(B))) \wedge \\
 & & (\#C > 0 \to isRrConfRes(last(C)))
\end{array}
$$

The assertion network for I_{er} is as follows:

$$
\begin{array}{lll}
Q_{s^i_{er}} & \stackrel{\text{def}}{=} & \#A = \#B = \#C = \#D = 0 \ \wedge \ |icTree \geqslant 2 \\
Q_{l_{i,1}} & \stackrel{\text{def}}{=} & \#A = \#B = \#C = \#D \ \wedge \ |icTree| \geqslant 2 \\
Q_{l_{i,2}} & \stackrel{\text{def}}{=} & \#B = \#C = \#D = (\#A - 1) \ \wedge \ last(A) = x_i \ \wedge \ |icTree| > 2 \wedge \\
 & & \quad isRrReq(last(A)) \ \wedge \ isUniquePID(last(A).spid) \wedge \\
 & & \quad isValidInd(last(A).cap)
\end{array}
$$

$$Q_{l_{i,3}} \stackrel{\text{def}}{=} \#B = \#C = \#D = (\#A - 1) \ \wedge \ last(A) = x_i \ \wedge \ |icTree| \geqslant 2 \wedge isValidInd(iIndCap) \ \wedge \ isTreeLocked$$

$$Q_{l_{i,5}} \stackrel{\text{def}}{=} \#B = \#C = \#D = (\#A - 1) \ \wedge \ last(A) = x_i \ \wedge \ |icTree| \geqslant 2 \wedge isRrReq(y_i) \ \wedge \ isUniquePID(y_i.spid) \ \wedge \ isValidInd(y_i.cap)$$

$$Q_{l_{i,6}} \stackrel{\text{def}}{=} \#B = \#D = (\#A - 1) = (\#C - 1) \ \wedge \ last(A) = x_i \ \wedge \ last(C) = y_i \wedge |icTree| \geqslant 2$$

$$Q_{l_{i,7}} \stackrel{\text{def}}{=} \#A = \#C = \#D = (\#B + 1) \ \wedge \ last(A) = x_i \ \wedge \ last(C) = y_i \wedge last(D) = z_i \ \wedge \ isRrConfRes(z_i) \ \wedge \ |icTree| \geqslant 2$$

$$Q_{l_{i,8}} \stackrel{\text{def}}{=} \#A = \#C = \#D = (\#B + 1) \ \wedge \ last(A) = x_i \ \wedge \ last(C) = y_i \wedge last(D) = z_i \ \wedge \ |icTree| \geqslant 2 \ \wedge \ isRrConfRes(w_i)$$

$$Q_{t^i_{er}} \stackrel{\text{def}}{=} false$$

We check the following implications to prove that the above assertion network is an A-C-inductive assertion network w.r.t. assumption Ass^i_{er}, commitment C^i_{er}, and channels A, B, C, and D.

- $\models Q_{s^i_{er}} \rightarrow C^i_{er}$ follows from the above definitions.
- $\models Q_{s^i_{er}} \ \wedge \ Ass^i_{er} \ \rightarrow \ Q_{l_{i,1}} \circ init^i_{er}$. In this internal transition, the size of the intermediate-capability tree does not change. Hence, this verification holds.
- $\models Q_{l_{i,1}} \ \wedge \ Ass^i_{er} \rightarrow ((Ass^i_{er} \rightarrow Q_{l_{i,2}}) \ \wedge \ C^i_{er}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x_i, \ h \mapsto v, \ \sigma(h).(A, v))$ for arbitrary value v. In this input transition, just communication through channel A took place, and function g assigns the received value to x_i. Since $\#A > 0$, the first implication of Ass^i_{er} satisfies $isRrReq(last(A))$, $isUniquePID(last(A).spid)$, and $isValidInd(last(A).cap)$. Furthermore, we have $\sigma' \models |icTree| > 2$ because $isValidInd(last(A).cap)$ indicates that there is an intermediate indicator in addition to the root and the parent capability inside the tree. Thus, this verification holds.
- $\models Q_{l_{i,2}} \ \wedge \ Ass^i_{er} \rightarrow Q_{l_{i,3}} \circ f_{i,1}$. In this internal transition, function $f_{i,1}$ copies the intermediate indicator inside the tree, which $last(A).cap$ points to it, removes it from the tree, and assigns the copied intermediate indicator to variable $iIndCap$ when it returns. Thus, this verification holds.
- $\models Q_{l_{i,3}} \ \wedge \ Ass^i_{er} \rightarrow Q_{l_{i,4}} \circ f_{i,2}$. In this internal transition, function $f_{i,2}$ creates a capability-revocation request for program R_{er} and assigns it to variable y_i, such that $isRrReq(y_i) = true$ and $y_i.spid = last(A).spid$. Furthermore, we have $isUniquePID(y_i.spid) = true$ because $isUniquePID(last(A).spid) = true$ and $y_i.spid = last(A).rpid$. In addition, this transition satisfies $isValidInd(y_i.cap)$ because we have $isValidInd(indCap)$ and $y_i.cap = indCap$. Thus, this verification holds.
- $\models Q_{l_{i,4}} \ \wedge \ Ass^i_{er} \rightarrow ((Ass^i_{er} \rightarrow Q_{l_{i,5}}) \ \wedge \ C^i_{er}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(C, \sigma(y_i)))$. In this output transition, program I_{er} sends y_i through channel

C. C^i_{er} holds because $last(C) = \sigma(y_i)$ and $isRrReq(y_i)$, $isUniquePID(y_i.spid)$, and $isValidInd(y_i.cap)$. Hence, this verification holds.

- $\models Q_{l_{i,5}} \wedge Ass^i_{er} \rightarrow ((Ass^i_{er} \rightarrow Q_{l_{i,6}}) \wedge C^i_{er}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : z_i,\ h \mapsto v,\ \sigma(h).(D, v))$ for arbitrary value v. In this input transition, a communication through channel D took place, and function g assigns the received value to z_i. Since $\#D > 0$, Ass^i_{er} implies that $\sigma' \models isRrConfRes(z_i)$. Thus, this verification holds.
- $\models Q_{l_{i,6}} \wedge Ass^i_{er} \rightarrow Q_{l_{i,7}} \circ f_{i,3}$. In this internal transition, function $f_{i,3}$ creates a external revocation-confirmation response for the process and assigns it to w_i such that $isRrConfRes(w_i)$. Hence, this verification holds.
- $\models Q_{l_{i,7}} \wedge Ass^i_{er} \rightarrow ((Ass^i_{er} \rightarrow Q_{l_{i,1}}) \wedge C^i_{er}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B, \sigma(w_i)))$. In this output transition, program I_{er} sends w_i through channel B. Commitment C^i_{er} holds because $\sigma \models isRrConfRes(w_i)$. Hence, this verification holds.

Since $Q_{t^i_{er}} \rightarrow \psi^i_{er}$, the post-condition of program I_{er} is satisfied.

5.7.2 External Revocation - Resource Controller

Program R_{er} receives a capability-revocation request from program I_{er} via channel B. In the next step, program R_{er} removes the delegated capability and all re-delegated capabilities in its sub-tree. Finally, it sends a revocation-confirmation response toward program I_{er}. The functions of R_{er} are defined as follow:

$$
\begin{aligned}
init^r_{er}(\sigma) &= (\sigma : rootPtr \mapsto getRoot(\sigma(icTree))),\\
f_{r,1}(\sigma) &= (\sigma : subtreeList \mapsto revoke(\sigma(rootPtr), \sigma(x_r.cap))),\\
f_{r,2}(\sigma) &= (\sigma : isListEmpty \mapsto checkList(\sigma(subtreeList))),\\
f_{r,3}(\sigma) &= (\sigma : nextCap \mapsto getNextCap(\sigma(subtreeList))),\\
f_{r,4}(\sigma) &= (\sigma : revokeCap(\sigma(nextCap))),\\
f_{r,5}(\sigma) &= (\sigma : y_r \mapsto genRevConfRes(\sigma(x_r)))
\end{aligned}
$$

The A-C formula for program R_{er} is as follows:

$$\vdash \langle Ass^r_{er},\ C^r_{er}\rangle\ \{\varphi^r_{er}\}\ R_{er}\ \{\psi^r_{er}\}$$

where the formal definition of φ^r_{er}, ψ^r_{er}, Ass^r_{er}, and C^r_{er} are as follows:

$$
\begin{aligned}
\varphi^r_{er} &\stackrel{\text{def}}{=} \#C = \#D = 0 \wedge |rcTree| \geqslant 1\\
\psi^r_{er} &\stackrel{\text{def}}{=} false\\
Ass^r_{er} &\stackrel{\text{def}}{=} \#C > 0 \rightarrow\\
&\quad (isRrReq(last(B)) \wedge isUniquePID(last(B).spid) \wedge\\
&\quad isValidInd(last(B).cap))
\end{aligned}
$$

$$C^r_{er} \quad \stackrel{\text{def}}{=} \quad \#C = \#D > 0 \rightarrow isRrConfRes(last(D))$$

The assertion network for R_{er} is as follows:

$$Q_{s^r_{er}} \stackrel{\text{def}}{=} \#C = \#D = 0 \ \wedge \ |rcTree \geqslant 2$$

$$Q_{l_{r,1}} \stackrel{\text{def}}{=} \#C = \#D \ \wedge \ |rcTree| \geqslant 2$$

$$Q_{l_{r,2}} \stackrel{\text{def}}{=} \#D = (\#C - 1) \ \wedge \ last(C) = x_r \ \wedge \ |rcTree| > 2 \wedge isRrReq(last(C)) \ \wedge \ isUniquePID(last(C).spid) \wedge isValidInd(last(C).cap)$$

$$Q_{l_{r,3}} \stackrel{\text{def}}{=} \#D = (\#C - 1) \ \wedge \ last(C) = x_r \ \wedge \ |rcTree| \geqslant 2$$

$$Q_{l_{r,4}} \stackrel{\text{def}}{=} \#D = (\#C - 1) \ \wedge \ last(C) = x_r \ \wedge \ |rcTree| \geqslant 2 \ \wedge \ \neg isListEmpty$$

$$Q_{l_{r,5}} \stackrel{\text{def}}{=} \#D = (\#C - 1) \ \wedge \ last(C) = x_r \ \wedge \ |rcTree| \geqslant 2 \ \wedge \ isListEmpty \wedge isRrConfRes(y_r)$$

$$Q_{t^r_{er}} \stackrel{\text{def}}{=} false$$

We check the following implications to prove that the above assertion network is an A-C-inductive assertion network w.r.t. assumption Ass^r_{er}, commitment C^r_{er}, and channels C and D.

- $\models Q_{s^r_{er}} \rightarrow C^r_{er}$ follows from the above definitions.
- $\models Q_{s^r_{er}} \ \wedge \ Ass^r_{er} \ \rightarrow \ Q_{l_{r,1}} \circ init^r_{er}$. In this internal transition, the size of the intermediate-capability tree does not change. Hence, this verification holds.
- $\models Q_{l_{r,1}} \ \wedge \ Ass^r_{er} \rightarrow ((Ass^r_{er} \rightarrow Q_{l_{r,2}}) \ \wedge \ C^r_{er}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x_r, \ h \mapsto v, \ \sigma(h).(C, v))$ for arbitrary value v. In this input transition, just communication through channel C took place, and function g assigns the received value to x_r. Since $\#C > 0$, the first implication of Ass^r_{er} satisfies $isRrReq(last(C))$, $isUniquePID(last(C).spid)$, and $isValidInd(last(C).cap)$. Furthermore, we have $\sigma' \models |rcTree| > 2$ because $isValidInd(last(C).cap)$ indicates that there is a delegated resource capability in addition to the root and the parent capability inside the tree. Thus, this verification holds.
- $\models Q_{l_{r,2}} \ \wedge \ \neg isListEmpty \ \wedge \ Ass^r_{er} \rightarrow Q_{l_{r,3}} \circ (f_{r,2} \circ f_{r,1})$. In this internal transition, function $f_{i,1}$ revokes the resource capability inside the tree, which $last(C).cap$ points to it. In addition, it returns the sub-tree of the resource capability as a list. Thus, we have $\sigma' \models |rcTree| \geqslant 2$. In the next step, function $f_{r,2}$ checks if the list is empty. Hence, this verification holds.
- $\models Q_{l_{r,3}} \ \wedge \ \neg isListEmpty \ \wedge \ Ass^r_{er} \rightarrow Q_{l_{r,4}} \circ (f_{r,4} \circ f_{r,3})$. In this internal transition, the $\neg isListEmpty$ condition implies that $\sigma' \models \neg isListEmpty$. Hence, function $f_{i,3}$ gets the next resource capability that program R_{er} should revokes . It assigns the next resource capability to variable $nextCap$. Thus, this verification holds.
- $\models Q_{l_{r,4}} \ \wedge \ Ass^r_{er} \rightarrow Q_{l_{r,3}} \circ f_{r,2}$. In this internal transition, function $f_{r,2}$ checks if the list is empty. Hence, this verification holds.

- $\models Q_{l_{r,3}} \wedge isListEmpty \wedge Ass^r_{er} \rightarrow Q_{l_{r,5}} \circ f_{r,5}$. In this internal transition, the $isListEmpty$ condition implies that $\sigma' \models isListEmpty$. Hence, function $f_{r,5}$ generates a revocation-confirmation response and assigns it to variable y_r. Hence, this verification holds.
- $\models Q_{l_{r,5}} \wedge Ass^r_{er} \rightarrow ((Ass^r_{er} \rightarrow Q_{l_{r,1}}) \wedge C^r_{er}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(D, \sigma(y_r)))$. In this output transition, program R_{er} sends y_r through channel D. Commitment C^r_{er} holds because $\sigma \models isRrConfRes(y_r)$. Hence, this verification holds.

Since $Q_{t^r_{er}} \rightarrow \psi^r_{er}$, the post-condition of program R_{er} is satisfied.

5.7.3 External Revocation - Parallel Composition

This section presents the parallel composition of the external-revocation components based on the described rule in 1. Consider the parallel composition $R_{er} \parallel I_{er}$. Program R_{er} satisfies the assumption-commitment pair $(Ass^r_{er},\ C^r_{er})$ as follows:

$$\vdash \langle Ass^r_{er},\ C^r_{er} \rangle\ \{\varphi^r_{er}\}\ R_{er}\ \{\psi^r_{er}\}$$

where the formal definition of φ^r_{er}, ψ^r_{er}, Ass^r_{er}, and C^r_{er} are as follows:

$$\begin{aligned}
\varphi^r_{er} &\stackrel{\text{def}}{=} \#C = \#D = 0 \wedge |rcTree| \geqslant 1 \\
\psi^r_{er} &\stackrel{\text{def}}{=} false \\
Ass^r_{er} &\stackrel{\text{def}}{=} \#C > 0 \rightarrow \\
&\quad (isRrReq(last(B)) \wedge isUniquePID(last(B).spid) \wedge \\
&\quad isValidInd(last(B).cap)) \\
C^r_{er} &\stackrel{\text{def}}{=} \#C = \#D > 0 \rightarrow isRrConfRes(last(D))
\end{aligned}$$

Program I_{er} satisfies the assumption-commitment pair $(Ass^i_{er},\ C^i_{er})$ as follows:

$$\vdash \langle Ass^i_{er},\ C^i_{er} \rangle\ \{\varphi^i_{er}\}\ I_{er}\ \{\psi^i_{er}\}$$

where the formal definition of φ^i_{er}, ψ^i_{er}, Ass^i_{er}, and C^i_{er} are as follows:

$$\begin{aligned}
\varphi^i_{er} &\stackrel{\text{def}}{=} \#A = \#B = \#C = \#D = 0 \wedge |icTree| \geqslant 1 \\
\psi^i_{er} &\stackrel{\text{def}}{=} false \\
Ass^i_{er} &\stackrel{\text{def}}{=} (\#A > 0 \rightarrow \\
&\quad isRrReq(last(A)) \wedge isUniquePID(last(A).spid))) \\
&\quad isValidInd(last(A).cap)) \wedge \\
&\quad (\#C = \#D > 0 \rightarrow isRrConfRes(last(D))) \\
C^i_{er} &\stackrel{\text{def}}{=} (\#A = \#B = \#C = \#D > 0 \rightarrow isRrConfRes(last(B))) \wedge \\
&\quad (\#C > 0 \rightarrow isRrConfRes(last(C)))
\end{aligned}$$

By applying the parallel composition rule, we deduce as follows:

$$\frac{\vdash \langle Ass_{er},\ C_{er}\rangle}{\{\varphi_{er}\}\ R_{er} \parallel I_{er}\ \{\psi_{er}\}}$$

where the formal definition of φ_{er}, ψ_{er}, Ass_{er}, and C_{er} are as follows:

$$\begin{array}{lll}
\varphi_{er} & \stackrel{\text{def}}{=} & \#A = \#B = \#C = \#D = 0 \ \wedge\ |rcTree| \geqslant 1 \ \wedge \\
 & & |icTree| \geqslant 1 \\
\psi_{er} & \stackrel{\text{def}}{=} & false \\
Ass_{er} & \stackrel{\text{def}}{=} & \#A > 0 \rightarrow \\
 & & (isRrReq(last(A)) \ \wedge\ isUniquePID(last(A).spid) \wedge \\
 & & isValidInd(last(A).cap)) \\
C_{er} & \stackrel{\text{def}}{=} & \#A = \#B = \#C = \#D > 0 \rightarrow isRrConfRes(last(B))
\end{array}$$

□

5.8 Fifth Lemma: Internal Revocation

The fifth lemma indicates that the internal revocation of a valid p-cap by the delegator process will invalidate the delegated p-cap to another process inside the same node. Furthermore, the revocation operation encompasses all the re-delegated capabilities from the first delegated capability. Consequently, the resource controller participates in the internal-revocation operation if one of the re-delegations includes a external delegation. We formally define the lemma and proof it.

Lemma 5. *Given a process with a unique PID in a process node, an intermediate controller in the same node, and a resource controller inside a resource node, revoking a delegated p-cap to another process inside the same node invalidates the delegated p-cap and all its internal and external re-delegations.*

Proof. We use the assumption-commitment technique to prove the lemma.

When a process receives a internally delegated capability, it may perform a internal or external re-delegation. This re-delegation can include both internal and external delegations. Hence, the intermediate and resource controllers must participate in revoking the delegated capability and all the re-delegated capability in its sub-tree. To perform the revocation, program Ir collects the delegated capabilities in a list. Then, it iterates through the list and revokes the capabilities.

We model the intermediate controller at the delegating-process side and the resource controllers in a external-revocation operation by programs $I_{rr} \stackrel{\text{def}}{=} (L^i_{ir}, T^i_{ir}, s^i_{ir}, t^i_{ir})$

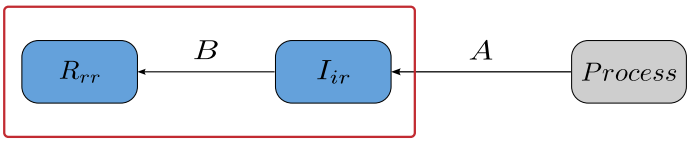


Figure 14: Syntactic Interfaces of the Internal-revocation Programs.

and $R_{rr} \stackrel{\text{def}}{=} (L^r_{rr}, T^r_{rr}, s^r_{rr}, t^r_{rr})$, respectively. The programs and the process exchange messages via synchronous channels to handle internal-revocation and possible external-revocation requests. Figure 12 depicts these two programs and their syntactic interfaces. Program R_{rr} operates as explained in 5.7.1. Figures 15 and 13b illustrate sequential diagrams of programs I_{ir} and R_{rr}, respectively. In the next step, we prove that when the process sends a internal-revocation request, programs I_{ir} and R_{rr} revoke the delegated capability along with all the re-delegated capabilities in its sub-tree.

Program I_{ir} receives a internal capability-revocation request from program P_{ir} via channel A and removes the delegated capability and all its internal or external re-delegated capabilities from the capability tree with the participation of the resource controller. Finally, it returns revocation confirmation response to the process via channel B. The conditions and functions of I_{ir} are as follows:

$$
\begin{aligned}
init^i_{ir}(\sigma) &= (\sigma : rootPtr, isListEmpty \mapsto \\
&\qquad getRoot(\sigma(icTree), true)), \\
f_{i,1}(\sigma) &= (\sigma : capsList \mapsto \\
&\qquad getDelegatedCapsList(\sigma(rootPtr), \sigma(x_i.cap))), \\
f_{i,2}(\sigma) &= (\sigma : isListEmpty \mapsto IsCapsListEmpty(\sigma(capsList))), \\
f_{i,3}(\sigma) &= (\sigma : nextCap \mapsto getNextCap(\sigma(capsList)), \\
f_{i,4}(\sigma) &= (\sigma : isIndCap \mapsto isIndCapability(\sigma(nextCap))), \\
f_{i,5}(\sigma) &= (\sigma : revokeCap(\sigma(nextCap))), \\
f_{i,6}(\sigma) &= (\sigma : iIndCap \mapsto revokeInd(\sigma(nextCap))), \\
f_{i,7}(\sigma) &= (\sigma : y_i \mapsto genRrReq(\sigma(x_i), \sigma(iIndCap))), \\
f_{i,8}(\sigma) &= (\sigma : w_i \mapsto genRevConfRes(\sigma(z_i))))
\end{aligned}
$$

The A-C formula for program I_{ir} is as follows:

$$\vdash \langle Ass^i_{ir},\ C^i_{ir} \rangle\ \{\varphi^i_{ir}\}\ I_{ir}\ \{\psi^i_{ir}\}$$

The formal definition of φ^i_{ir}, ψ^i_{ir}, As^i_{ir}, and C^i_{ir} are as follows:

$$
\begin{aligned}
\varphi^i_{ir} &\stackrel{\text{def}}{=} \#A = \#B = \#C = \#D = 0\ \wedge\ |icTree| \geqslant 1 \\
\psi^i_{ir} &\stackrel{\text{def}}{=} false \\
Ass^i_{ir} &\stackrel{\text{def}}{=} (\#A > 0 \rightarrow \\
&\qquad isLrReq(last(A))\ \wedge\ isValidInd(last(A).cap))) \wedge
\end{aligned}
$$

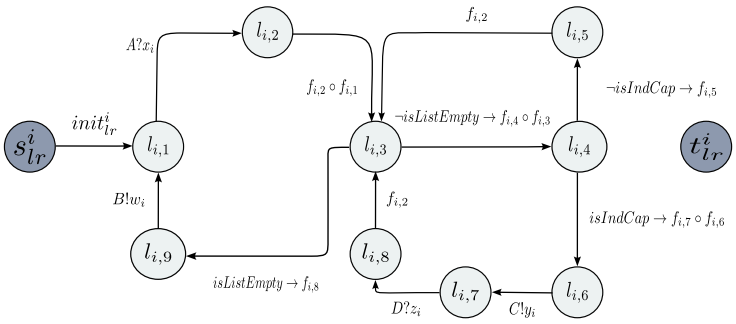


Figure 15: Internal Revocation - Program I_{ir}.

$$C^i_{ir} \quad \stackrel{\text{def}}{=} \quad (\#C = \#D > 0 \to isRrConfRes(last(D))) \\ \#A = \#B > 0 \to isLrConfRes(last(B))$$

The assertion network for I_{ir} is as follows:

$$Q_{s^i_{ir}} \stackrel{\text{def}}{=} \#A = \#B = \#C = \#D = 0 \ \wedge \ |icTree| \geqslant 1$$

$$Q_{l_{i,1}} \stackrel{\text{def}}{=} \#A = \#B = \#C = \#D \ \wedge \ isListEmpty$$

$$Q_{l_{i,2}} \stackrel{\text{def}}{=} \#B = \#C = \#D = (\#A - 1) \ \wedge \ last(A) = x_i \ \wedge \ isLrReq(last(A)) \wedge \\ isUniquePID(last(A).spid) \ \wedge \ isValidInd(last(A).cap) \ \wedge \ isListEmpty$$

$$Q_{l_{i,3}} \stackrel{\text{def}}{=} \#B = \#C = \#D = (\#A - 1) \ \wedge \ last(A) = x_i$$

$$Q_{l_{i,4}} \stackrel{\text{def}}{=} \#B = \#C = \#D = (\#A - 1) \ \wedge \ last(A) = x_i \ \wedge \ \neg isListEmpty$$

$$Q_{l_{i,5}} \stackrel{\text{def}}{=} \#B = \#C = \#D = (\#A - 1) \ \wedge \ last(A) = x_i \ \wedge \ \neg isIndCap$$

$$Q_{l_{i,6}} \stackrel{\text{def}}{=} \#B = \#C = \#D = (\#A - 1) \ \wedge \ last(A) = x_i \wedge \\ isIndCap \ \wedge \ isValidInd(iIndCap) \\ isRrReq(y_i) \ \wedge \ isUniquePID(y_i.spid) \ \wedge \ isValidInd(y_i.cap)$$

$$Q_{l_{i,7}} \stackrel{\text{def}}{=} \#B = \#D = (\#A - 1) = (\#C - 1) \ \wedge \ last(A) = x_i \ \wedge \ last(C) = y_i$$

$$Q_{l_{i,8}} \stackrel{\text{def}}{=} \#A = \#C = \#D = (\#B + 1) \ \wedge \ last(A) = x_i \ \wedge \ last(C) = y_i \ \wedge \ l \\ ast(D) = z_i \ \wedge \ isRrConfRes(z_i)$$

$$Q_{l_{i,9}} \stackrel{\text{def}}{=} \#B = \#C = \#D = (\#A - 1) \ \wedge \ last(A) = x_i \ \wedge \ isListEmpty \ \wedge \ isLrConfRes(z_i)$$

We check the following implications to prove that the above assertion network is an A-C-inductive assertion network w.r.t. assumption Ass^i_{ir}, commitment C^i_{ir}, and channels A, B, C, and D.

- $\models Q_{s^i_{ir}} \to C^i_{ir}$ follows from the above definitions.

- $\models Q_{s^i_{ir}} \wedge Ass^i_{ir} \rightarrow Q_{l_{i,1}} \circ init^i_{ir}$. In this internal transition, function $init^i_{ir}$ just assigns *true* to variable *isListEmpty*. Hence, this verification holds.
- $\models Q_{l_{i,1}} \wedge Ass^i_{ir} \rightarrow ((Ass^i_{ir} \rightarrow Q_{l_{i,2}}) \wedge C^i_{ir}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x_i,\ h \mapsto v,\ \sigma(h).(A, v))$ for arbitrary value v. In this input transition, just communication through channel A took place, and function g assigns the received value to x_i. Since $\#A > 0$, the first implication of Ass^i_{ir} satisfies $isLrReq(last(A))$, $isUniquePID(last(A).spid)$, and $isValidInd(last(A).cap)$. Thus, this verification holds.
- $\models Q_{l_{i,2}} \wedge Ass^i_{ir} \rightarrow Q_{l_{i,3}} \circ (f_{i,2} \circ f_{i,1})$. In this internal transition, function $f_{i,1}$ initialize the variable *capsList* with the delegated capability, which $last(A).cap$ points to it, and all the re-delegated capabilities in its sub-tree. Afterward, function $f_{i,2}$ checks if the list is empty. Thus, this verification holds.
- $\models Q_{l_{i,3}} \wedge \neg isListEmpty \wedge Ass^i_{ir} \rightarrow Q_{l_{i,4}} \circ (f_{i,4} \circ f_{i,3})$. In this internal transition, the condition implies that there is another capability in the list that the intermediate controller should revoke it. Function $f_{i,3}$ extracts this capability from the list, and function $f_{i,4}$ checks if it is a externally delegated capability. Hence, this verification holds.
- $\models Q_{l_{i,4}} \wedge \neg isIndCap \wedge Ass^i_{ir} \rightarrow Q_{l_{i,5}} \circ f_{i,5}$. The condition implies that the intermediate controller can revoke it internally in this internal transition. Hence, function $f_{i,5}$ revokes the capability internally by invalidating and removing it from the capability tree. Thus, this verification holds.
- $\models Q_{l_{i,5}} \wedge Ass^i_{ir} \rightarrow Q_{l_{i,3}} \circ f_{i,2}$. In this internal transition, function $f_{i,2}$ checks if the list is empty. Hence, this verification holds.
- $\models Q_{l_{i,4}} \wedge isIndCap \wedge Ass^i_{ir} \rightarrow Q_{l_{i,6}} \circ (f_{i,7} \circ f_{i,6})$. The condition indicates that the intermediate and resource controller should collaborate because it is a externally delegated capability. Hence, function $f_{i,6}$ copies the intermediate indicator capability, removes it from the tree, and assigns the copied intermediate indicator to variable *iIndCap* when it returns. Afterward, function $f_{i,7}$ creates a capability-revocation request for program R_{rr} and assigns it to variable y_i, such that $isRevReq(y_i) = true$ and $y_i.spid = last(A).spid$. In addition, $\sigma' \models isUniquePID(y_i.spid)$ because it is equal to the receiving process id from the process, and Ass^i_{ir} implies that $isUniquePID(last(A).spid)$ Thus, this verification holds.
- $\models Q_{l_{i,6}} \wedge Ass^i_{ir} \rightarrow ((Ass^i_{ir} \rightarrow Q_{l_{i,7}}) \wedge C^i_{ir}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(C, \sigma(y_i)))$. In this output transition, program I_{ir} sends y_i through channel C. C^i_{ir} holds because $last(C) = \sigma(y_i)$, and from $Q_{l_{i,7}}$, we have $isRevReq(y_i)$, $isUniquePID(y_i.spid)$, and $isValidInd(y_i.cap)$. Hence, this verification holds.
- $\models Q_{l_{i,7}} \wedge Ass^i_{ir} \rightarrow ((Ass^i_{ir} \rightarrow Q_{l_{i,8}}) \wedge C^i_{ir}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : z_i,\ h \mapsto v,\ \sigma(h).(D, v))$ for arbitrary value v. In this input transition, a communication through channel D took place, and function g assigns the received value to z_i. Since $\#D > 0$, Ass^i_{ir} implies that $\sigma' \models isRrConfRes(z_i)$. Thus, this verification holds.
- $\models Q_{l_{i,8}} \wedge Ass^i_{ir} \rightarrow Q_{l_{i,3}} \circ f_{i,2}$. In this internal transition, function $f_{i,2}$ checks if the list is empty. Hence, this verification holds.

- $\models Q_{l_{i,3}} \wedge isListEmpty \wedge Ass^i_{ir} \rightarrow Q_{l_{i,9}} \circ (f_{i,8} \circ unlockTree)$. In this internal transition, the condition implies that the intermediate controller has revoked all the delegated capabilities from the list. Afterward, function $f_{i,8}$ creates a revocation-confirmation response for the process and assigns it to w_i such that $isLrConfRes(w_i)$. Thus, this verification holds.
- $\models Q_{l_{i,9}} \wedge Ass^i_{ir} \rightarrow ((Ass^i_{ir} \rightarrow Q_{l_{i,1}}) \wedge C^i_{ir}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B, \sigma(w_i)))$. In this output transition, program I_{ir} sends w_i through channel B. Commitment C^i_{ir} holds because $\sigma \models isLrConfRes(w_i)$. Hence, this verification holds.

Since $Q_{t^i_{ir}} \rightarrow \psi^i_{ir}$, the post-condition of program I_{ir} is satisfied.

5.8.1 Internal Revocation - Parallel Composition

This section presents the parallel composition of the external-revocation components based on the described rule in 1. Consider the parallel composition $R_{rr} \parallel I_{ir}$. Program R_{rr} satisfies the assumption-commitment pair $(Ass^r_{rr},\ C^r_{rr})$ as follows:

$$\vdash \langle Ass^r_{rr},\ C^r_{rr}\rangle\ \{\varphi^r_{rr}\}\ R_{rr}\ \{\psi^r_{rr}\}$$

where the formal definition of φ^r_{rr}, ψ^r_{rr}, Ass^r_{rr}, and C^r_{rr} are as follows:

$$\begin{aligned}
\varphi^r_{rr} &\stackrel{\text{def}}{=} \#C = \#D = 0 \wedge |rcTree| \geqslant 1\\
\psi^r_{rr} &\stackrel{\text{def}}{=} false\\
Ass^r_{rr} &\stackrel{\text{def}}{=} \#C > 0 \rightarrow\\
&\quad (isRrReq(last(B)) \wedge isUniquePID(last(B).spid) \wedge\\
&\quad isValidInd(last(B).cap))\\
C^r_{rr} &\stackrel{\text{def}}{=} \#C = \#D > 0 \rightarrow isRrConfRes(last(D))
\end{aligned}$$

Program I_{rr} satisfies the assumption-commitment pair $(Ass^i_{ir},\ C^i_{ir})$ as follows:

$$\vdash \langle Ass^i_{ir},\ C^i_{ir}\rangle\ \{\varphi^i_{ir}\}\ I_{ir}\ \{\psi^i_{ir}\}$$

The formal definition of φ^i_{ir}, ψ^i_{ir}, As^i_{ir}, and C^i_{ir} are as follows:

$$\begin{aligned}
\varphi^i_{ir} &\stackrel{\text{def}}{=} \#A = \#B = \#C = \#D = 0 \wedge |icTree| \geqslant 1\\
\psi^i_{ir} &\stackrel{\text{def}}{=} false\\
Ass^i_{ir} &\stackrel{\text{def}}{=} (\#A > 0 \rightarrow\\
&\quad isLrReq(last(A)) \wedge isValidInd(last(A).cap))) \wedge\\
&\quad (\#C = \#D > 0 \rightarrow isRrConfRes(last(D)))\\
C^i_{ir} &\stackrel{\text{def}}{=} \#A = \#B > 0 \rightarrow isLrConfRes(last(B))
\end{aligned}$$

By applying the parallel composition rule, we deduce as follows:

$$\frac{\vdash \langle Ass_{ir},\ C_{ir}\rangle}{\{\varphi_{ir}\}\ R_{ir} \parallel I_{ir}\ \{\psi_{ir}\}}$$

where the formal definition of φ_{ir}, ψ_{ir}, Ass_{ir}, and C_{ir} are as follows:

$$\begin{array}{lll}
\varphi_{ir} & \stackrel{\text{def}}{=} & \#A = \#B = \#C = \#D = 0\ \wedge\ |rcTree| \geqslant 1 \wedge \\
 & & |icTree| \geqslant 1 \\
\psi_{ir} & \stackrel{\text{def}}{=} & false \\
Ass_{ir} & \stackrel{\text{def}}{=} & \#A > 0 \rightarrow \\
 & & (isLrReq(last(A))\ \wedge\ isValidInd(last(A).cap)) \\
C_{ir} & \stackrel{\text{def}}{=} & (\#A = \#B > 0 \wedge \#C = \#D > 0) \rightarrow \\
 & & isLrConfRes(last(B))
\end{array}$$

□

5.8.2 Capability Safety

Capability safety implies that a process can only obtain its capabilities through a resource allocation or a capability delegation and only employ its valid capabilities.

Definition 1. *Capability System. A capability system is a tuple comprising the following:*

- *a capability set* $\mathbb{C} = \{\mathbb{C}_r \cup \mathbb{C}_i \cup \mathbb{C}_p\}$*;*
- *a function:* $rsrc\colon \mathbb{C} \rightarrow \mathbb{R}$
- *a function:* $priv\colon \mathbb{C} \rightarrow 2^{\mathbb{V}}$
- *a function:* $pCaps\colon \mathbb{P} \rightarrow 2^{\mathbb{C}_p}$
- *a function:* $cAuth\colon \mathbb{C} \rightarrow \mathbb{R} \times 2^{\mathbb{V}}$
- *a function:* $pAuth\colon \mathbb{P} \rightarrow 2^{\mathbb{R}} \times 2^{\mathbb{V}}$

The tuple must satisfy the following conditions to denote a valid capability system: $\forall\ c_p \in \mathbb{C}_p, c_i \in \mathbb{C}_i, c_r \in \mathbb{C}_r, T_i \in \mathbb{T}_i,$ *and* $T_r \in \mathbb{T}_r$

(a) $c_p \mapsto c_i \Rightarrow cAuth(c_p) \subseteq cAuth(c_i)$

(b) $c_i \mapsto c_r \Rightarrow cAuth(c_i) \subseteq cAuth(c_r)$

(c) $isInTree(T_i, c_i, c_i') \Rightarrow cAuth(c_i') \subseteq cAuth(c)\ \ s.t.\ \ c_i \neq c_i^{root}$

(d) $isInTree(T_r, c_r, c_r') \Rightarrow cAuth(c_r') \subseteq cAuth(c_r)$

The valid-capability set of a process indicates the legitimately acquired capabilities by the process that are still valid; thus, the process can employ them for read/write operations. We formally define this set as follows:

$$validCaps(p) \subseteq pCaps(p)\text{: } (\forall c_p \in pCaps(p) \;\; s.t. \\ isValidProCap(c_p) \Rightarrow c_p \in validCaps(p))$$

Now, we define the capability-safety property and prove that our capability-based access-control system is capability safe.

Definition 2. *Capability Safety. An access-control system is capability safe, concerning the capability system* $(\mathbb{C}, rsrc, priv, pCap, cAuth, pAuth)$*, if the following condition holds for all processes* $p \in \mathbb{P}$:

- $rsrcSet(p) = \bigcup_{c_p \in validCaps(p)} rsrc(c_p)$

Where $rsrcSet$ indicates accessible resources by the process.

Proof. The proof proceeds by induction on the structure of the process's capability set. The proof consists of one base case and two inductive cases.

- **Base Case:** The capability set is empty.
  In this case, the process possesses no valid capability; thus, the process can access no resources.
- **Inductive Case One:** $validCaps(p)$ contains the current process's valid capabilities; hence, we have:

  $$rsrcSet(p) = \bigcup_{c_p \in validCaps(p)} rsrc(c_p)$$

  Based on Lemmas 1 to 3, the process receives a valid process capability, c_p^{new}, due to a resource-allocation or internal/external-delegation request. Its valid-capability set changes as follows:

  $$validCaps'(p) = validCaps(p) \cup c_p^{new}$$

  Hence, its new resource list transforms as follows:

  $$rsrcSet'(p) = rsrcSet(p) \cup rsrc(c_p^{new})$$

- **Inductive Case Two:** $validCaps(p)$ contains the current process's valid capabilities; hence, we have:

  $$rsrcSet(p) = \bigcup_{c_p \in validCaps(p)} rsrc(c_p)$$

  Based on Lemmas 4 to 5, one of the process's capabilities, c_p^{old}, becomes invalid due to an internal/external revocation. Its valid-capability set changes as follows:

$$validCaps'(p) = validCaps(p) \setminus c_p^{old}$$

Thus, its new resource list transforms as follows:

$$rsrcSet'(p) = rsrcSet(p) \setminus rsrc(c_p^{old})$$

□

5.8.3 Authority Safety

We claim that a distributed capability-based access-control system is authority safe if it addresses the following properties regarding the object-capability model:

- **An authority's owner obtained it through a capability delegation**: A process can acquire authority only if the owner of the authority delegates it to the process.
- **No authority amplification**: The capability owners can only delegate what authority they have.

Our access-control system guarantees both properties. Processes can only obtain capabilities through allocating resources or delegating capabilities by other processes. Furthermore, using well-formed capability trees, the access-control system ensures that no process can delegate an authority it does not own. We define the authority-safety property as follows:

Definition 3. *Authority Safety. A capability-based access-control system is authority safe, concerning the capability system* ($\mathbb{C}$, $rsrc$, $priv$, $pCap$, $cAuth$, $pAuth$)*, if the following condition holds for all processes* $p \in \mathbb{P}$:[1]

- $$pAuth(p) = \bigcup_{c_p \in validCaps(p)} cAuth(c_p)$$

Proof. The proof proceeds by induction on the structure of the process's capability set. The proof consists of one base case and two inductive cases.

- **Base Case:** The capability set is empty.
  In this case, the process possesses no valid capability; thus, the process can access no resources.
- **Inductive Case One:** $validCaps(p)$ contains the current process's valid capabilities; hence, we have:

  $$rsrcSet(p) = \bigcup_{c_p \in validCaps(p)} rsrc(c_p)$$

  Based on Lemmas 1 to 3, the process receives a valid process capability, c_p^{new}, due to a resource-allocation or internal/external-delegation request. Its valid-capability set changes as follows:

  $$validCaps'(p) = validCaps(p) \cup c_p^{new}$$

Hence, its authority transforms as follows:

$$pAuth'(p) = pAuth(p) \cup cAuth(c_p^{new})$$

In addition, because all the capability trees are well-formed, the authority of the delegated capability is always a subset of the orginal capability.

- **Inductive Case Two:** $validCaps(p)$ contains the current process's valid capabilities; hence, we have:

$$rsrcSet(p) = \bigcup_{c_p \in validCaps(p)} rsrc(c_p)$$

Based on Lemmas 4 to 5, one of the process's capabilities, c_p^{old}, becomes invalid due to an internal/external revocation. Its valid-capability set changes as follows:

$$validCaps'(p) = validCaps(p) \setminus c_p^{old}$$

Thus, its authority transforms as follows:

$$pAuth'(p) = pAuth(p) \setminus pAuth(c_p^{old})$$

□

5.9 Isolation Property

The isolation property expresses that two processes cannot access to the same resource. This property guarantees that untrusted processes cannot access trusted processes' resources. We formally define this property as follows:

Definition 4. *Isolation Property. Given a set of Resources* $R \subseteq \mathbb{R}$ *and a set of processes* $p_1, \cdots, p_k \in P \subseteq \mathbb{P}$*, we have* $Isolation(R, p_1, \cdots, p_k \in P)$ *if*:

- $\forall\, i, j\colon (1 \leqslant i < j \leqslant k \;\wedge\; rsrcSet(p_i) \subseteq R \;\wedge\; rsrcSet(p_i) \subseteq R)$
  $\Rightarrow\; rsrcSet(p_i) \cap rsrcSet(p_j) = \emptyset$

Processes can isolate their resources by delegating no capability. However, this approach is error-prone because it relies on developers to ensure processes never delegate their capabilities. Therefore, we support the isolation automatically using new permission. Let $\mathbb{Y} = \{d\}$ be the capability-related permission set, where d denotes the delegation permission. When controllers generate capabilities due to allocating resources, they unset this permission. Thus, because processes cannot delegate their capabilities and our capability-based access-control system is capability and authority safe, it supports the isolation property.

Proof. The proof proceeds by induction on the structure of capability trees.

we start with the resource capability. The proof consists of one base case and three inductive cases.

- **Base Case:** The capability set is empty.
  In this case, the resource capability tree only contain the root capability; thus, it satisfies the isolation property.
- **Inductive Case One:** The capability contains more than one capability and it satisfies the isolation property. The resource controller receives a resource-allocation request. Based on 1–**??** the resource controller allocates the resource which is free and adds its corresponding resource capability to tree. Furthermore, it unset the delegation permission, d, in the resource capability. Because the new capability does not have any overlap with the existing ones, the tree satisfies the isolation property. Moreover, it creates the corresponding intermediate capability, in which the delegation permission is unset.
- **Inductive Case Two:**The capability contains more than one capability and it satisfies the isolation property. The resource controller receives a external-delegation request. Because the delegation permission is unset in all the resource capabilities inside the tree, the resource controller rejects the request and does not change the tree. Thus, the tree satisfies the isolation property.
- **Inductive Case Three:** The capability contains more than one capability and it satisfies the isolation property. The resource controller receives a external-revocation request. However, because the delegation permission is unset in all the capabilities inside the tree, none of them have a delegation-hierarchy as its sub-tree. Thus, the resource controller reject the request because the intermediate capability inside the request points to an non-existing resource capability. Therefore, the tree does not change and it satisfies the isolation property.

Now, we proof the isolation property for the intermediate tree. The proof consists of one base case and three inductive cases.

- **Base Case:** The capability set is empty.
  In this case, the intermediate capability tree only contain the root capability; thus, it satisfies the isolation property.
- **Inductive Case One:** The capability contains more than one capability and it satisfies the isolation property. The intermediate controller receives a resource-allocation response and inserts it as the direct child of the tree's root. Because the resource in the received intermediate capability does not have overlap with any resources in the resource node, it does not have overlap with any capability in the resource node. Thus, it does not have any overlap with the existing intermediate capability inside the intermediate tree. Thus, the tree satisfies the isolation property.
- **Inductive Case Two:**The capability contains more than one capability and it satisfies the isolation property. The intermediate controller receives a internal-delegation request. Because the delegation permission is unset in all the intermediate capabilities inside the tree, the intermediate controller rejects the request and does not change the tree. Thus, the tree satisfies the isolation property.
- **Inductive Case Three:** The capability contains more than one capability and it satisfies the isolation property. The resource controller receives a internal-delegation request. However, because the delegation permission is unset in all the

capabilities inside the intermediate tree, none of them have a delegation-hierarchy as its sub-tree. Thus, the resource controller reject the request because the process capability inside the request points to an non-existing intermediate capability. Hence, the tree does not change and it satisfies the isolation property.

Therefore, we proved that our access-control system supports the isolation property. □

6 Use Case

MDC [35] provides direct access to the shared memory pool. The direct access to the shared memory introduces a vulnerability to the MDC's architecture. For example, imagine a process that uses the shared memory pool as the communication medium due to its direct and memory-speed persistence access; the process writes data on the shared memory and passes the data's reference to another process to communicate with it. However, a third process can read the communicated data by knowing the reference and violate the security or privacy of data. Therefore, MDC requires an access-control system to preserve the security and privacy of data in the shared memory pool.

We instantiates our capability-based access-control system for MDC as the use case and demonstrate how it handles requests and capabilities[1]. In our general-purpose system, programs directly connect to other programs via synchronous channels (as depicted in Figure 6). However, in MDC, they are part of the instantiated controllers. An instantiated controller integrates all the related components inside the controller and connects them to the rest of the system via *handler*s and bridges. In addition, we add a module to OS which connects processes to the intermediate controller. We assume adversaries cannot compromise this module. This section describes describes nodes and controllers in the instantiated system, their components, and their syntactic interfaces. Furthermore, we explain how they cooperate to control access.

The new components change the environments of the existing components. In addition, new components commit to guaranteeing some of the previous assumptions. For example, the OS module checks the process ID in a request against the sender's PID because processes may act maliciously. Thus, it commits that each request contains a unique process ID, and it belongs to the sender. To prove the soundness of the instantiated system, we verify that it guarantees security properties. Thus, because the proofs of the properties depend on Lemmas 1 to 5, we must refine lemmas' proofs.

To refine Lemmas' proofs, we first verify the new modules regarding the assumption-commitment method. Afterward, we instantiate controllers by integrating the verified modules and applying the parallel composition rule (Rule 1). The soundness of the parallel composition rule depends on the validity of the A-C formulas of the integrated modules and the validity of the hypothesis of Rule 1 ($A \wedge C_1 \rightarrow A_2$, $A \wedge C_2 \rightarrow A_1$) for the joint channels between modules [17]. Finally, we verify the lemmas; thus, we prove that the instantiated system guarantees the security properties. Section *Use Case* of the Technical Report represents the whole proof.

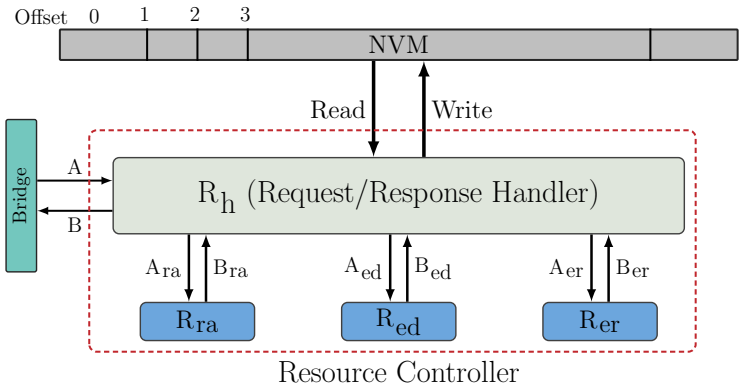
6.1 Resource Node

Figure 16a depicts a resource node in the instantiated system, including a resource controller and a byte-addressable NVM.

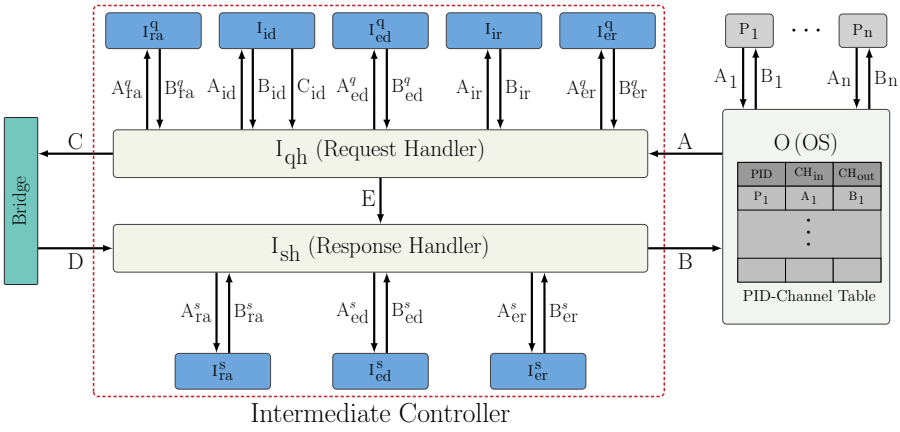
6.1.1 Resource Controller

The instantiated resource controller comprises four components: Request/Response handler (program R_h), Resource Allocation (R_{ra}), External Delegation (R_{ed}), and Ex-

[1] **??** contains the capability structures of the instantiated system.



(a) Resource Node's Components and their Syntactic Interfaces.



(b) PE Node's Components and their Syntactic Interfaces.

Figure 16: Instantiated Access-Control System for MDC.

ternal Revocation (R_{er}). Each component has its assumptions and commitments. We define program R as the parallel execution of the programs in the controller as follows:

$$R \stackrel{\text{def}}{=} R_h \parallel R_{ra} \parallel R_{ed} \parallel R_{er}$$

With the A-C formula $\vdash \langle A^r, C^r \rangle : \{\varphi^r\} R \{\psi^r\}$. By applying the parallel composition rule, the commitments of the controller should be the commitments of all its components ($C_h \wedge C_{ra} \wedge C_{ed} \wedge C_{er}$). Furthermore, we should check the correctness of the controller's assumptions by checking the validity of the hypothesis ($A \wedge C_1 \rightarrow A_2$, $A \wedge C_2 \rightarrow A_1$) in Rule 1. It means, the controller's assumption and the handler's commitments should guarantee the assumption of programs R_{ra} (A_{ra}), R_{ed} (A_{ed}), and R_{er} (A_{er}).

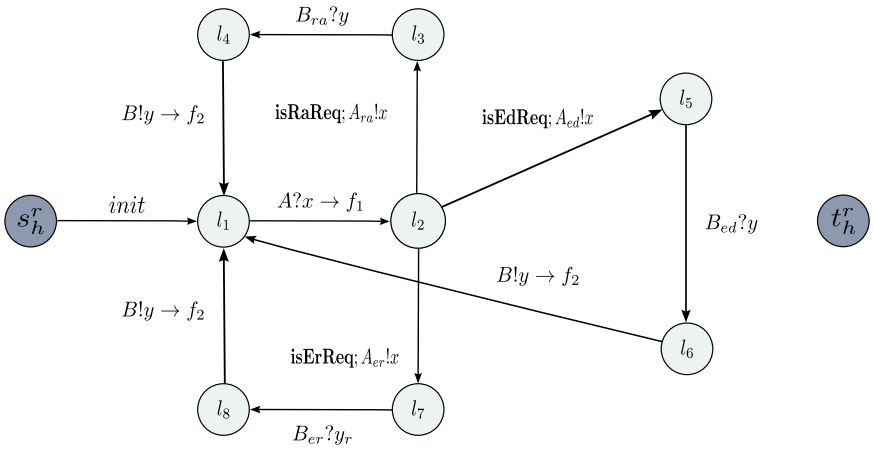


Figure 17: Request/Response-Handler Program of the Resource Controller.

6.1.1.1 Request/Response Handler

We model the request/response Handler by program $R_h \stackrel{\text{def}}{=} (L_h^r, T_h^r, s_h^r, t_h^r)$. Program R_h receives requests from channel A and processes them in a *First In / First Out* (FIFO) order. It checks each request and commits to forwarding the request to the corresponding program. Program R_h assumes that each received request contain a unique process ID in the sender's PE node. Because each request contains a unique process ID and program R_h commits to forwarding it to the right program, which satisfies the programs' assumptions ($A^r \wedge C_h \rightarrow A_{ra,ed,er}$). Furthermore, these programs commit to returning valid responses (C_{ra}, C_{ed}, C_{er}). Thus, combining these commitments and assumption of channel A ($A^r \wedge C_{ra,ed,er}$) guarantees that R_h will receive valid responses, which it will send out through channel D. Therefore, the resource controller commits to return valid responses via channel D when it receives requests containing unique process IDs from channel A. Figure 17 depicts the state diagram of program R_h. The conditions and functions of program R_h are as follows:

$$
\begin{aligned}
init(\sigma) &= (\sigma : isRaReq,\ isEdReq,\ isErReq \mapsto false,\ false,\ false),\\
f_1(\sigma) &= (\sigma : isRaReq,\ isEdReq,\ isErReq \mapsto\\
&\qquad isRaReqCheck(\sigma(x)),\ isEdReqCheck(\sigma(x)),\ isErReqCheck(\sigma(x))),\\
f_2(\sigma) &= (\sigma : isRaReq,\ isEdReq,\ isErReq \mapsto false,\ false,\ false)
\end{aligned}
$$

The A-C formula for process R_{ra} is as follows:

$$\vdash \langle A_h^r\ C_h^r \rangle\ \{\varphi_h^r\}\ R_h\ \{\psi_h^r\}$$

where the formal definition of φ_r, ψ_r , A_{ra}^r, and C_{ra}^r are as follows:

$$\varphi_h^r \stackrel{\text{def}}{=} \#A = \#B = \#A_{ra} = \#B_{ra} = \#A_{ed} = \#B_{ed} = \#A_{er} = \#B_{er} = 0 \wedge$$

$$\neg isRaReq \ \wedge \ \neg isEdReq \ \wedge \ \neg isErReq$$

$$\psi_h^r \stackrel{\text{def}}{=} false$$

$$\begin{aligned} A_h^r \stackrel{\text{def}}{=} \ & (\#A > 0 \rightarrow isUniquePID(last(A).spid)) \\ & ((\#A_{ra} = \#B_{ra} > 0) \rightarrow isValidCap(last(B_{ra}).cap)) \wedge \\ & ((\#A_{ed} = \#B_{ed} > 0) \rightarrow isValidCap(last(B_{ed}).cap)) \wedge \\ & ((\#A_{er} = \#B_{er} > 0) \rightarrow isValidCap(last(B_{er}).cap)) \end{aligned}$$

$$\begin{aligned} C_h^r \stackrel{\text{def}}{=} \ & (\#A = \#B > 0) \rightarrow isValidCap(last(B).cap)) \wedge \\ & ((\#A_{ra} > 0 \ \wedge \ \#A_{ra} \neq \#B_{ra}) \rightarrow isUniquePID(last(A_{ra}).spid)) \wedge \\ & ((\#A_{ed} > 0 \ \wedge \ \#A_{ed} \neq \#B_{ed}) \rightarrow isUniquePID(last(A_{ed}).spid)) \wedge \\ & ((\#A_{er} > 0 \ \wedge \ \#A_{er} \neq \#B_{er}) \rightarrow isUniquePID(last(A_{er}).spid)) \end{aligned}$$

The assertion network for R_h is as follows:

$$\begin{aligned} Q_{s_h} \stackrel{\text{def}}{=} \ & \#A = \#B = 0 \ \wedge \ \#A_{ra} = \#B_{ra} = 0 \ \wedge \ \#A_{ed} = \#B_{ed} = 0 \ \wedge \ \#A_{er} = \#B_{er} = 0 \wedge \\ & \neg isRaReq \ \wedge \ \neg isEdReq \ \wedge \ \neg isErReq \end{aligned}$$

$$\begin{aligned} Q_1 \stackrel{\text{def}}{=} \ & \#A = \#B \ \wedge \ \#A_{ra} = \#B_{ra} \ \wedge \ \#A_{ed} = \#B_{ed} \ \wedge \ \#A_{er} = \#B_{er} \wedge \\ & \neg isRaReq \ \wedge \ \neg isEdReq \ \wedge \ \neg isErReq \end{aligned}$$

$$\begin{aligned} Q_2 \stackrel{\text{def}}{=} \ & (\#A - 1) = \#B \ \wedge \ \#A_{ra} = \#B_{ra} \ \wedge \ \#A_{ed} = \#B_{ed} \ \wedge \ \#A_{er} = \#B_{er} = 0 \wedge \\ & \neg isRaReq \ \wedge \ \neg isEdReq \ \wedge \ \neg isErReq \wedge \\ & last(A) = x \ \wedge isUniquePID(last(A).spid) \end{aligned}$$

$$\begin{aligned} Q_3 \stackrel{\text{def}}{=} \ & (\#A - 1) = \#B \ \wedge \ (\#A_{ra} - 1) = \#B_{ra} \ \wedge \ \#A_{ed} = \#B_{ed} \ \wedge \ \#A_{er} = \#B_{er} \wedge \\ & isRaReq \ \wedge \ \neg isEdReq \ \wedge \ \neg isErReq \ \wedge \ last(A_{ra}) = x \end{aligned}$$

$$\begin{aligned} Q_4 \stackrel{\text{def}}{=} \ & (\#A - 1) = \#B \ \wedge \ \#A_{ra} = \#B_{ra} \ \wedge \ \#A_{ed} = \#B_{ed} \ \wedge \ \#A_{er} = \#B_{er} \wedge \\ & isRaReq \ \wedge \ \neg isEdReq \ \wedge \ \neg isErReq \wedge \\ & last(B_{ra}) = y \ \wedge \ isValidCap(last(B_{ra}).cap) \end{aligned}$$

$$\begin{aligned} Q_5 \stackrel{\text{def}}{=} \ & (\#A - 1) = \#B \ \wedge \ \#A_{ra} = \#B_{ra} \ \wedge \ (\#A_{ed} - 1) = \#B_{ed} \ \wedge \ \#A_{er} = \#B_{er} \wedge \\ & \neg isRaReq \ \wedge \ isEdReq \ \wedge \ \neg isErReq \ \wedge \ last(A_{ed}) = x \end{aligned}$$

$$\begin{aligned} Q_6 \stackrel{\text{def}}{=} \ & (\#A - 1) = \#B \ \wedge \ \#A_{ra} = \#B_{ra} \ \wedge \ \#A_{ed} = \#B_{ed} \ \wedge \ \#A_{er} = \#B_{er} \wedge \\ & \neg isRaReq \ \wedge \ isEdReq \ \wedge \ \neg isErReq \wedge \\ & last(B_{ed}) = y \ \wedge \ isValidCap(last(B_{ed}).cap) \end{aligned}$$

$$\begin{aligned} Q_7 \stackrel{\text{def}}{=} \ & (\#A - 1) = \#B \ \wedge \ \#A_{ra} = \#B_{ra} \ \wedge \ \#A_{ed} = \#B_{ed} \ \wedge \ (\#A_{er} - 1) = \#B_{er} \wedge \\ & \neg isRaReq \ \wedge \ \neg isEdReq \ \wedge \ isErReq \ \wedge \ last(A_{er}) = x \end{aligned}$$

$$\begin{aligned} Q_8 \stackrel{\text{def}}{=} \ & (\#A - 1) = \#B \ \wedge \ \#A_{ra} = \#B_{ra} \ \wedge \ \#A_{ed} = \#B_{ed} \ \wedge \ \#A_{er} = \#B_{er} \wedge \\ & \neg isRaReq \ \wedge \ \neg isEdReq \ \wedge \ isErReq \wedge \end{aligned}$$

$$last(B_{er}) = y \ \wedge \ isValidCap(last(B_{er}).cap)$$

$$Q_{tr_{ra}^r} \stackrel{\text{def}}{=} false$$

We check the following implications to prove that the above assertion network is an A-C-inductive assertion network w.r.t. assumption A_h^r, commitment C_h^r, and channels A, B, A_{ra}, B_{ra}, A_{ed}, B_{ed}, A_{er}, and B_{er}.

- $\models Q_{s_h^r} \rightarrow C_h^r$ follows from the above definitions.
- $\models Q_{s_h^r} \wedge A_h^r \rightarrow Q_{l_1} \circ init$. In this internal transition, function *init* does unset boolean variables $isRaReq$, $isEdReq$, and $isErReq$. Hence, this verification holds.
- $\models Q_{l_1} \wedge A_h^r \rightarrow ((A_h^r \rightarrow Q_{l_2}) \wedge C_h^r) \circ (f_1 \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x, h \mapsto v, \sigma(h).(A, v))$ for arbitrary v. In this input transition, a communication through channel A just took place. Function g assigns the last received value from channel A to x. Because $\#A > 0$, the first implication of A_h^r satisfies $isUniquePID(last(A).spid)$ predicate. Function f_1 checks the variable x to find the request type and assigns boolean variables $isRaReq$, $isEdReq$, and $isErReq$ accordingly. Thus, this verification holds.
- $\models Q_{l_2} \ \wedge \ isRaReq \ \wedge \ A_h^r \rightarrow ((A_h^r \rightarrow Q_{l_3}) \ \wedge \ C_h^r) \circ (g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A_{ra}, \sigma(x)))$. In this output transition, program R_h sends x through channel A_{ra} toward program R_{ra}. From the transition's condition we have $isRaReq$. C_h^r holds because $\#A_{ra} > 0 \ \wedge \ \#A_{ra} \neq \#B_{ra}$ and $\sigma \models isUniquePID(x.spid)$. Hence, this verification holds.
- $\models Q_{l_3} \wedge A_h^r \rightarrow ((A_h^r \rightarrow Q_{l_4}) \wedge C_h^r) \circ (g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : y, h \mapsto v, \sigma(h).(B_{ra}, v))$ for arbitrary v. In this input transition, a communication through channel B_{ra} just took place and function g assigns the last received value to y. Because $\#A_{ra} = \#B_{ra} > 0$, the second implication of A_h^r satisfies $isValidCap(last(B_{ra}).cap)$. Thus, this verification holds.
- $\models Q_{l_4} \wedge A_h^r \rightarrow ((A_h^r \rightarrow Q_{l_1}) \wedge C_h^r) \circ (f_2 \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B, \sigma(y)))$. In this output transition, program R_h just sends out variable y through channel B. Furthermore, function f_2 does unset boolean variables $isRaReq$, $isEdReq$, and $isErReq$. C_h^r holds because $\#A = \#B > 0$, and $\sigma \models isValidCap(y.cap)$. Hence, this verification holds.
- $\models Q_{l_2} \ \wedge \ isEdReq \ \wedge \ A_h^r \rightarrow ((A_h^r \rightarrow Q_{l_5}) \ \wedge \ C_h^r) \circ (g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A_{ed}, \sigma(x)))$. In this output transition, program R_h sends x through channel A_{ed} toward program R_{ed}. From the transition's condition we have $isEdReq$. C_h^r holds because $\#A_{ed} > 0 \ \wedge \ \#A_{ed} \neq \#B_{ed}$ and $\sigma \models isUniquePID(x.spid)$. Hence, this verification holds.
- $\models Q_{l_5} \wedge A_h^r \rightarrow ((A_h^r \rightarrow Q_{l_6}) \wedge C_h^r) \circ (g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x, h \mapsto v, \sigma(h).(B_{ed}, v))$ for arbitrary v. In this input transition, a communication through channel B_{ed} just took place and function g assigns the last received value to y. Because $\#A_{ed} = \#B_{ed} > 0$, the second implication of A_h^r satisfies $isValidCap(last(B_{ed}).cap)$. Thus, this verification holds.
- $\models Q_{l_6} \wedge A_h^r \rightarrow ((A_h^r \rightarrow Q_{l_1}) \wedge C_h^r) \circ (f_2 \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B, \sigma(y)))$. In this output transition, program R_h just sends out variable y through channel B.

Furthermore, function f_2 does unset boolean variables *isRaReq*, *isEdReq*, and *isErReq* C_h^r holds because $\#A = \#B > 0$, and $\sigma \models isValidCap(y.cap)$. Hence, this verification holds.

- $\models Q_{l_2} \wedge isEdReq \wedge A_h^r \rightarrow ((A_h^r \rightarrow Q_{l_7}) \wedge C_h^r) \circ (g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A_{er}, \sigma(x)))$. In this output transition, program R_h sends x through channel A_{er} toward program R_{ed}. From the transition's condition we have $isErReq.\ C_h^r$ holds because $\#A_{er} > 0 \wedge \#A_{er} \neq \#B_{ed}$ and $\sigma \models isUniquePID(x.spid)$. Hence, this verification holds.
- $\models Q_{l_7} \wedge A_h^r \rightarrow ((A_h^r \rightarrow Q_{l_8}) \wedge C_h^r) \circ (g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x, h \mapsto v, \sigma(h).(B_{er}, v))$ for arbitrary v. In this input transition, a communication through channel B_{er} just took place and function g assigns the last received value to y. Because $\#A_{er} = \#B_{er} > 0$, the second implication of A_h^r satisfies $isValidCap(last(B_{er}).cap)$. Thus, this verification holds.
- $\models Q_{l_8} \wedge A_h^r \rightarrow ((A_h^r \rightarrow Q_{l_1}) \wedge C_h^r) \circ (f_2 \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B, \sigma(y)))$. In this output transition, program R_h just sends out variable y through channel B. Furthermore, function f_2 does unset boolean variables *isRaReq*, *isEdReq*, and *isErReq* C_h^r holds because $\#A = \#B > 0$, and $\sigma \models isValidCap(y.cap)$. Hence, this verification holds.

Since $Q_{t_h^r} \rightarrow \psi_h^r$, the post-condition of program R_h is satisfied.

6.2 PE Node

Figure 16b illustrates a PE node in the instantiated system, comprising an intermediate controller, an operating system (OS), and running processes in the node.

6.2.1 Operating System

OS acts as a mediator between processes and the intermediate controller. We model the operating system in the PE node by program $O \stackrel{\text{def}}{=} (L^o, T^o, s^o, t^o)$. It has two tasks: assigning unique *ID*/communication channels to each process and forwarding received messages to appropriate channels. Program O employs a table (*PID-Channel*) to map process *ID*s to in/out channels (Figure 16b). Therefore, it can check if the process *ID* in a request belongs to the sender. Furthermore, O forwards received responses to processes.

Program O commits to the intermediate controller that the *PID* in a request belongs to the sender and is unique inside the node by performing the first task and checking requests against the table. Furthermore, it commits to processes that they will receive their valid responses using the table.

Program O receives a resource-allocation request from process p_i via channel A_i and checks the request. If the check passes, the program forwards the request toward program I through channel A. Otherwise, it returns an error message to program P_i. In addition, It receives the response from program I via channel B, finds the appropriate channel, and sends the response to program p_j through this channel. Figure 18 depicts the state diagram of program O. The conditions and functions of program O are as follows:

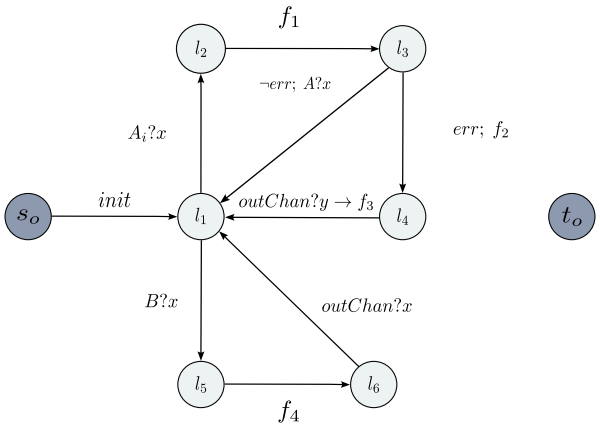


Figure 18: Program of the Operating System.

$$
\begin{aligned}
init(\sigma) &= (\sigma : tablePtr \mapsto getTablePtr(\sigma(OSTable))),\\
f_1(\sigma) &= (\sigma : err \mapsto checkIsUniquePID(\sigma(x), tablePtr)),\\
f_2(\sigma) &= (\sigma : y, outChan \mapsto createErrResponse(\sigma(x))),\\
f_3(\sigma) &= (\sigma : err \mapsto false),\\
f_4(\sigma) &= (\sigma : outChan, \mapsto findChannel(\sigma(x), tablePtr)),
\end{aligned}
$$

where $OSTable$ is the $PID - channel$ table of the operating system

The A-C formula for process O is as follows:

$$\vdash \langle A^o,\ C^o \rangle :\ \{\varphi^o\}\ O\ \{\psi^o\}$$

where the formal definition of φ^o, ψ^o , A^o, and C^o are as follows:

$$
\begin{aligned}
\varphi^o &\stackrel{\text{def}}{=} \#A = \#B = 0\ \wedge\ \neg err\ \wedge\ \#outChan = 0\\
\psi^o &\stackrel{\text{def}}{=} false\\
A^o &\stackrel{\text{def}}{=} \#B > 0 \rightarrow isValidCap(last(B).cap)\\
C^o &\stackrel{\text{def}}{=} (\#A > 0 \rightarrow\ isUniquePID(last(A).spid)) \wedge\\
&\qquad ((\#outChan > 0\ \wedge\ \neg err) \rightarrow\ isValidCap(last(outChan).cap))
\end{aligned}
$$

Where $outChannel$ is a logical variable.

The assertion network for O is as follows:

$$
\begin{aligned}
Q_{s_o} &\stackrel{\text{def}}{=} \#A = \#B = 0\ \wedge\ \neg err\ \wedge\ \#outChan = 0\\
Q_1 &\stackrel{\text{def}}{=} \neg err
\end{aligned}
$$

$$Q_2 \stackrel{\text{def}}{=} \neg err \wedge last(A_i.spid) = x$$

$$Q_3 \stackrel{\text{def}}{=} last(A_i.spid) = x$$

$$Q_4 \stackrel{\text{def}}{=} err$$

$$Q_5 \stackrel{\text{def}}{=} last(B) = x \wedge \neg err \wedge isValidCap(last(B).cap)$$

$$Q_6 \stackrel{\text{def}}{=} last(B) = x \wedge isValidCap(x.cap)) \wedge \neg err$$

$$Q_{t_o} \stackrel{\text{def}}{=} false$$

We check the following implications to prove that the above assertion network is an A-C-inductive assertion network w.r.t. assumption A^o, commitment C^o, and channels A, B, A_i, B_i such that $1 \leqslant i \leqslant n$.

- $\models Q_{s_o} \rightarrow C^o$ follows from the above definitions.
- $\models Q_{s_o} \wedge A^o \rightarrow Q_{l_1} \circ init$. In this internal transition, function *init* just assign a pointer to the table to variable *tablePtr* and $\sigma \models \neg err$. Hence, this verification holds.
- $\models Q_{l_1} \wedge A^o \rightarrow ((A^o \rightarrow Q_{l_2}) \wedge C^o) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x,\ h \mapsto v,\ \sigma(h).(A_i, v))$ for arbitrary v. In this input transition, a communication through channel A_i, such that $1 \leqslant i \geqslant n$, just took place. Function g assigns the last received value from channel A_i to x. Thus, this verification holds.
- $\models Q_{l_2} \wedge A^o \rightarrow (A^o \rightarrow Q_{l_3}) \circ f_1$. In this internal transition, function f_1 checks the request to see if it is unique in the node and assign the result to variable *err* Thus, this verification holds.
- $\models Q_{l_3} \wedge \neg err \wedge A^o \rightarrow ((A^o \rightarrow Q_{l_1}) \wedge C^o) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A, \sigma(x)))$. In this output transition, program O just sends out variable x through channel A. The condition of the transition states that there is no error, which means the process ID in the request is unique. Therefore, commitment C^o is satisfied. Hence, this verification holds.
- $\models Q_{l_3} \wedge err \wedge A^o \rightarrow (A^o \rightarrow Q_{l_4}) \circ f_2$. In this internal transition, the condition of the transition states that there is error. Furthermore, the commitment C^o is satisfied because $\sigma \models err$. Thus, this verification holds.
- $\models Q_{l_4} \wedge A^o \rightarrow ((A^o \rightarrow Q_{l_1}) \wedge C^o) \circ (f_3 \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(outChan, \sigma(y)))$. In this output transition, program O just sends out variable y through channel *outChan*. Because $\sigma \models err$, commitment C^o is satisfied. In addition, function f_1 does unset variable *err*. Hence, this verification holds.
- $\models Q_{l_1} \wedge A^o \rightarrow ((A^o \rightarrow Q_{l_5}) \wedge C^o) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x,\ h \mapsto v,\ \sigma(h).(B, v))$ for arbitrary v. In this input transition, a communication through channel B just took place and function g assigns the last received value to x. $\sigma' \models isValidCap(last(B).cap)$ Because $\#B > 0$, Thus, this verification holds.
- $\models Q_{l_5} \wedge A^o \rightarrow (A^o \rightarrow Q_{l_6}) \circ f_4$. In this internal transition, function f_4 finds the appropriate output channel and assigns it to *outChan*. Furthermore, x contains a

valid capability because it contains the last received message from channel B and $\sigma \models isValidCap(last(B).cap)$. Hence, this verification holds.

- $\models Q_{l_6} \wedge A^o \rightarrow ((A^o \rightarrow Q_{l_1}) \wedge C^o) \circ (f_3 \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(outChan, \sigma(x)))$. In this output transition, program O just sends out variable y through channel $outChan$. Because $\sigma \models \neg err \wedge isValidCap(x.cap)$, commitment C^o is satisfied. Thus, this verification holds.

Since $Q_{t^o} \rightarrow \psi^o$, the post-condition of program O is satisfied.

6.2.2 Intermediate Controller

We follow the pattern in which we reasoned about the resource controller to reason about the intermediate controller regarding the parallel composition rule. We model the intermediate controller by program I as the parallel execution of the above programs as follows:

$$I \stackrel{\text{def}}{=} I_{qh} \parallel I^q_{ra} \parallel I_{id} \parallel I^q_{ed} \parallel I_{ir} \parallel I^q_{er} \parallel I_{sh} \parallel I^s_{ra} \parallel I^s_{ed} \parallel I^s_{er}$$

With the A-C formula $\vdash \langle A^i, C^i \rangle : \{\varphi^i\}\ I\ \{\psi^i\}$, after applying the parallel composition rule. The commitments of the intermediate controller will be the combination of its programs. Assumption A^i indicates that the intermediate controller assumes the process ID inside each request is unique in the PE node, and responses from resource controllers contain valid capabilities. However, before checking the correctness of its assumptions, we describe how they cooperate to handle requests and responses.

The intermediate controller handles requests and responses in parallel via request and response handlers Each handler has three tasks: locking the capability tree, forwarding its input to the appropriate module, and sending the response of a module to the output channel. Parallel handling of requests and responses may cause manipulating the tree simultaneously, thus,breaking the tree's well-formedness The handlers employ a locking mechanism ($\mathscr{L}$) to lock the tree before processing each input to prevent the situation. We assume $\mathscr{L}$ performs the locking task correctly and fairly. Therefore, controllers can always guarantee the tree's well-formedness. We now explain how each handler accomplishes its task.

6.2.2.1 Request Handling

We model the request handler by the program I_{qh}. Program I_{qh} cooperates with five other programs to handle requests, including I^q_{ra} (resource-allocation request handler), I_{id} (the internal-delegation handler), I^q_{ed} (the external-delegation request handler), I_{ir} (the internal-revocation handler), and I^q_{er} (the external-revocation request handler). Program I_{qh} assumes that the PID in a request belongs to the sender and is unique inside the node. I_{qh} commits to forward the request to the corresponding program and forwarding programs' responses via output channels. Figure 19 depicts the state diagram of program I_{qh}.

Program I_{qh} receives requests of the processes inside a process node via channel A. It uses five predicates to find out the type of a request and forward the request to the

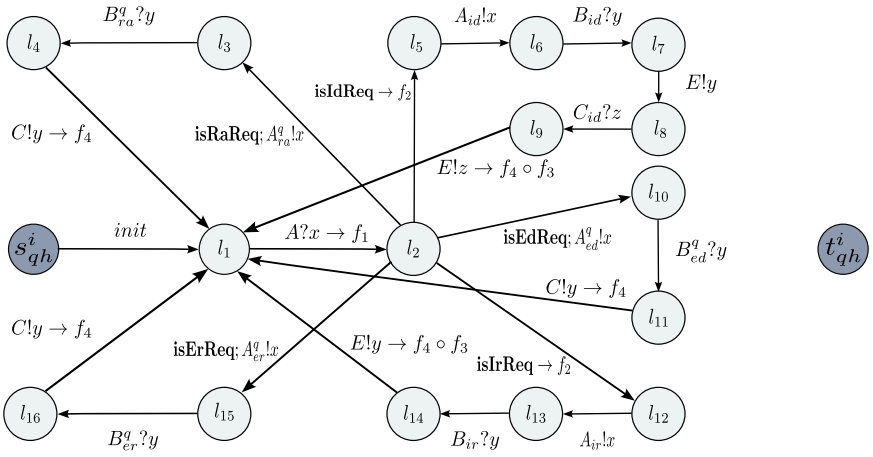


Figure 19: Request-Handler Program of the Intermediate Controller.

corresponding module. Then, the handler receives the response and forwards it to the appropriate channel. If the request is handled locally, the handler forwards the response to channel C_{12}. Otherwise, the handler forwards the response of the module to a remote resource node via channel B. The conditions and functions of I_{qh} are defined as follow:

$$
\begin{aligned}
init(\sigma) = \ & (\sigma : rootPtr, treeLocked, \\
& isRaReq,\ isIdReq,\ isEdReq,\ isIrReq,\ isErReq \mapsto \\
& getRoot(\sigma(icTree)),\ false,\ false,\ false,\ false,\ false,\ false), \\
f_1(\sigma) \ = \ & (\sigma : isRaReq,\ isIdReq,\ isEdReq,\ isIrReq,\ isErReq \mapsto \\
& isRaReqCheck(\sigma(x)),\ isIdReqCheck(\sigma(x)),\ isEdReqCheck(\sigma(x)), \\
& isIrReqCheck(\sigma(x)),\ isErReqCheck(\sigma(x))), \\
f_2(\sigma) \ = \ & (\sigma : treeLocked \mapsto lockTree(\sigma(rootPtr))), \\
f_3(\sigma) \ = \ & (\sigma : treeLocked \mapsto unlockTree(\sigma(rootPtr))), \\
f_4(\sigma) \ = \ & (\sigma : isRaReq,\ isIdReq,\ isEdReq,\ isIrReq,\ isErReq \mapsto \\
& false,\ false,\ false,\ false,\ false)
\end{aligned}
$$

The A-C formula for process I_{qh} is as follows:

$$\vdash \langle A^i_{qh}\ C^i_{qh} \rangle\ \{\varphi^i_{qh}\}\ I_{qh}\ \{\psi^i_{qh}\}$$

where the formal definition of φ^i_{qh}, ψ^i_{qh} , A^i_{qh}, and C^i_{qh} are as follows:

$$
\begin{aligned}
\varphi^i_{qh} \stackrel{\text{def}}{=} \ & \#A = \#C = \#E = 0 \ \wedge\ \#A^q_{ra} = \#B^q_{ra} = 0 \ \wedge\ \#A_{id} = \#B_{id} = \#C_{id} = 0 \ \wedge \\
& \#A^q_{ed} = \#B^q_{ed} = 0 \ \wedge\ \#A_{ir} = \#B_{ir} = 0 \ \wedge\ \#A^q_{er} = \#B^q_{er} = 0 \\
\psi^i_{qh} \stackrel{\text{def}}{=} \ & false
\end{aligned}
$$

$$
\begin{aligned}
A^i_{qh} \stackrel{\text{def}}{=}\ & (\#A > 0 \rightarrow isUniquePID(last(A).spid)) \\
& ((\#B^q_{ra} > 0) \rightarrow isUniquePID(last(B^q_{ra}).spid)) \\
& ((\#B_{id} > 0) \rightarrow isValidCap(last(B_{id}).cap)) \wedge \\
& ((\#C_{id} > 0) \rightarrow isIdConfRes(last(C_{id}).cap)) \wedge \\
& ((\#B^q_{ed} > 0) \rightarrow isUniquePID(last(B^q_{ed}).spid)) \wedge \\
& ((\#B_{ir} > 0) \rightarrow isIrConfRes(last(B_{ir}))) \wedge \\
& ((\#B^q_{er} > 0) \rightarrow isUniquePID(last(B^q_{er}).spid))
\end{aligned}
$$

$$
\begin{aligned}
C^i_{qh} \stackrel{\text{def}}{=}\ & (\#C > 0) \rightarrow isUniquePID(last(C).spid)) \wedge \\
& (\#E > 0 \ \wedge\ isIrReq \rightarrow isIrConfRes(last(E))) \wedge \\
& (\#E > 0 \ \wedge\ \neg isIrReq) \rightarrow isValidCap(last(E).cap)) \wedge \\
& ((\#A^q_{ra} > 0 \ \wedge\ \#A_{ra} \neq \#B_{ra}) \rightarrow isUniquePID(last(A^q_{ra}).spid) \wedge \\
& isRaReq(last(A^q_{ra})) \wedge \\
& ((\#A_{id} > 0) \rightarrow isUniquePID(last(A_{id}).spid)) \wedge \\
& isIdReq(last(A_{ir})) \wedge \\
& ((\#A^q_{ed} > 0) \rightarrow isUniquePID(last(A^q_{ed}).spid)) \wedge \\
& isEdReq(last(A^q_{ed})) \wedge \\
& ((\#A_{ir} > 0) \rightarrow isUniquePID(last(A_{ir}).spid)) \wedge \\
& isIrReq(last(A_{ir})) \wedge \\
& ((\#A^q_{er} > 0) \rightarrow isUniquePID(last(A^q_{er}).spid)) \\
& isErReq(last(A^q_{er}))
\end{aligned}
$$

The assertion network for I_{qh} is as follows:

$$
\begin{aligned}
Q_{s^i_{qh}} \stackrel{\text{def}}{=}\ & \#A = \#C = \#E = 0 \ \wedge\ \#A^q_{ra} = \#B^q_{ra} = 0 \ \wedge\ \#A_{id} = \#B_{id} = \#C_{id} = 0 \wedge \\
& \#A^q_{ed} = \#B^q_{ed} = 0 \ \wedge\ \#A_{ir} = \#B_{ir} = 0 \ \wedge\ \#A^q_{er} = \#B^q_{er} = 0
\end{aligned}
$$

$$
\begin{aligned}
Q_1 \stackrel{\text{def}}{=}\ & \#A^q_{ra} = \#B^q_{ra} \ \wedge\ \#A_{id} = \#B_{id} = \#C_{id} \ \wedge\ \#A^q_{ed} = \#B^q_{ed} \ \wedge\ \#A_{ir} = \#B_{ir} \wedge \\
& \#A^q_{er} = \#B^q_{er} \ \wedge\ \neg treeLocked \wedge \\
& \neg isRaReq \ \wedge\ \neg isIdReq \ \wedge\ \neg isEdReq \ \wedge\ \neg isIrReq \ \wedge\ \neg isErReq
\end{aligned}
$$

$$
\begin{aligned}
Q_2 \stackrel{\text{def}}{=}\ & \#A^q_{ra} = \#B^q_{ra} \ \wedge\ \#A_{id} = \#B_{id} = \#C_{id} \ \wedge\ \#A^q_{ed} = \#B^q_{ed} \ \wedge\ \#A_{ir} = \#B_{ir} \wedge \\
& \#A^q_{er} = \#B^q_{er} \ \wedge\ \neg treeLocked \ \wedge\ last(A) = x \ \wedge\ isUniquePID(last(A).spid)
\end{aligned}
$$

$$
\begin{aligned}
Q_3 \stackrel{\text{def}}{=}\ & (\#A^q_{ra} - 1) = \#B^q_{ra} \ \wedge\ \#A_{id} = \#B_{id} = \#C_{id} \ \wedge\ \#A^q_{ed} = \#B^q_{ed} \ \wedge\ \#A_{ir} = \#B_{ir} \wedge \\
& \#A^q_{er} = \#B^q_{er} \ \wedge\ \neg treeLocked \ \wedge\ last(A) = x \ \wedge\ last(A^q_{ra}) = x \wedge \\
& isRaReq \ \wedge\ \neg isIdReq \ \wedge\ \neg isEdReq \ \wedge\ \neg isIrReq \ \wedge\ \neg isErReq
\end{aligned}
$$

$$
\begin{aligned}
Q_4 \stackrel{\text{def}}{=}\ & \#A^q_{ra} = \#B^q_{ra} \ \wedge\ \#A_{id} = \#B_{id} = \#C_{id} \ \wedge\ \#A^q_{ed} = \#B^q_{ed} \ \wedge\ \#A_{ir} = \#B_{ir} \wedge \\
& \#A^q_{er} = \#B^q_{er} \ \wedge\ \neg treeLocked \ \wedge\ last(A) = x \wedge \\
& last(A^q_{ra}) = x \ \wedge\ last(B^q_{ra}) = y \ \wedge\ isUniquePID(last(B^q_{ra}).spid)
\end{aligned}
$$

$$isRaReq \wedge \neg isIdReq \wedge \neg isEdReq \wedge \neg isIrReq \wedge \neg isErReq$$

$$Q_5 \stackrel{\text{def}}{=} \#A^q_{ra} = \#B^q_{ra} \wedge \#A_{id} = \#B_{id} = \#C_{id} \wedge \#A^q_{ed} = \#B^q_{ed} \wedge \#A_{ir} = \#B_{ir} \wedge$$
$$\#A^q_{er} = \#B^q_{er} \wedge treeLocked \wedge last(A) = x \wedge isUniquePID(last(A).spid) \wedge$$
$$\neg isRaReq \wedge isIdReq \wedge \neg isEdReq \wedge \neg isIrReq \wedge \neg isErReq$$

$$Q_6 \stackrel{\text{def}}{=} \#A^q_{ra} = \#B^q_{ra} \wedge (\#A_{id} - 1) = \#B_{id} = \#C_{id} \wedge \#A^q_{ed} = \#B^q_{ed} \wedge \#A_{ir} = \#B_{ir} \wedge$$
$$\#A^q_{er} = \#B^q_{er} \wedge treeLocked \wedge last(A) = x \wedge last(A_{id}) = x \wedge$$
$$\neg isRaReq \wedge isIdReq \wedge \neg isEdReq \wedge \neg isIrReq \wedge \neg isErReq$$

$$Q_7 \stackrel{\text{def}}{=} \#A^q_{ra} = \#B^q_{ra} \wedge \#A_{id} = \#B_{id} = (\#C_{id} + 1) \wedge \#A^q_{ed} = \#B^q_{ed} \wedge \#A_{ir} = \#B_{ir} \wedge$$
$$\#A^q_{er} = \#B^q_{er} \wedge treeLocked \wedge last(A) = x \wedge last(A_{id}) = x \wedge$$
$$last(B_{id}) = y \wedge isValidCap(last(B_{id}).cap) \wedge$$
$$\neg isRaReq \wedge isIdReq \wedge \neg isEdReq \wedge \neg isIrReq \wedge \neg isErReq$$

$$Q_8 \stackrel{\text{def}}{=} \#A^q_{ra} = \#B^q_{ra} \wedge \#A_{id} = \#B_{id} = (\#C_{id} + 1) \wedge \#A^q_{ed} = \#B^q_{ed} \wedge \#A_{ir} = \#B_{ir} \wedge$$
$$\#A^q_{er} = \#B^q_{er} \wedge treeLocked \wedge last(A) = x \wedge last(A_{id}) = x \wedge last(B_{id}) = y \wedge$$
$$\neg isRaReq \wedge isIdReq \wedge \neg isEdReq \wedge \neg isIrReq \wedge \neg isErReq$$

$$Q_9 \stackrel{\text{def}}{=} \#A^q_{ra} = \#B^q_{ra} \wedge \#A_{id} = \#B_{id} = (\#C_{id} + 1) \wedge \#A^q_{ed} = \#B^q_{ed} \wedge \#A_{ir} = \#B_{ir} \wedge$$
$$\#A^q_{er} = \#B^q_{er} \wedge treeLocked \wedge last(A) = x \wedge last(A_{id}) = x \wedge last(B_{id}) = y \wedge$$
$$last(C_{id}) = z \wedge isValidCap(last(C_{id}).cap) \wedge$$
$$\neg isRaReq \wedge isIdReq \wedge \neg isEdReq \wedge \neg isIrReq \wedge \neg isErReq$$

$$Q_{10} \stackrel{\text{def}}{=} \#A^q_{ra} = \#B^q_{ra} \wedge \#A_{id} = \#B_{id} = \#C_{id} \wedge (\#A^q_{ed} - 1) = \#B^q_{ed} \wedge \#A_{ir} = \#B_{ir} \wedge$$
$$\#A^q_{er} = \#B^q_{er} \wedge \neg treeLocked \wedge last(A) = x \wedge last(A^q_{ed}) = x \wedge$$
$$\neg isRaReq \wedge \neg isIdReq \wedge isEdReq \wedge \neg isIrReq \wedge \neg isErReq$$

$$Q_{11} \stackrel{\text{def}}{=} \#A^q_{ra} = \#B^q_{ra} \wedge \#A_{id} = \#B_{id} = \#C_{id} \wedge \#A^q_{ed} = \#B^q_{ed} \wedge \#A_{ir} = \#B_{ir} \wedge$$
$$\#A^q_{er} = \#B^q_{er} \wedge \neg treeLocked \wedge last(A) = x \wedge$$
$$last(A^q_{ed}) = x \wedge last(B^q_{ed}) = y \wedge isUniquePID(last(B^q_{ed}).spid)$$
$$\neg isRaReq \wedge \neg isIdReq \wedge isEdReq \wedge \neg isIrReq \wedge \neg isErReq$$

$$Q_{12} \stackrel{\text{def}}{=} \#A^q_{ra} = \#B^q_{ra} \wedge \#A_{id} = \#B_{id} = \#C_{id} \wedge \#A^q_{ed} = \#B^q_{ed} \wedge \#A_{ir} = \#B_{ir} \wedge$$
$$\#A^q_{er} = \#B^q_{er} \wedge treeLocked \wedge last(A) = x \wedge isUniquePID(last(A).spid) \wedge$$
$$\neg isRaReq \wedge \neg isIdReq \wedge \neg isEdReq \wedge isIrReq \wedge \neg isErReq$$

$$Q_{13} \stackrel{\text{def}}{=} \#A^q_{ra} = \#B^q_{ra} \wedge \#A_{id} = \#B_{id} = \#C_{id} \wedge \#A^q_{ed} = \#B^q_{ed} \wedge (\#A_{ir} - 1) = \#B_{ir} \wedge$$
$$\#A^q_{er} = \#B^q_{er} \wedge treeLocked \wedge last(A) = x \wedge last(A_{ir}) = x \wedge$$
$$\neg isRaReq \wedge \neg isIdReq \wedge \neg isEdReq \wedge isIrReq \wedge \neg isErReq$$

$$Q_{14} \stackrel{\text{def}}{=} \#A^q_{ra} = \#B^q_{ra} \wedge \#A_{id} = \#B_{id} = \#C_{id} \wedge \#A^q_{ed} = \#B^q_{ed} \wedge \#A_{ir} = \#B_{ir} \wedge$$
$$\#A^q_{er} = \#B^q_{er} \wedge treeLocked \wedge last(A) = x \wedge last(A_{ir}) = x \wedge$$
$$last(B_{ir}) = y \wedge isIrConfRes(last(B_{ir})) \wedge$$

$$\neg isRaReq \ \wedge \ \neg isIdReq \ \wedge \ \neg isEdReq \ \wedge \ isIrReq \ \wedge \ \neg isErReq$$

$$Q_{15} \stackrel{\text{def}}{=} \#A^q_{ra} = \#B^q_{ra} \ \wedge \ \#A_{id} = \#B_{id} = \#C_{id} \ \wedge \ \#A^q_{ed} = \#B^q_{ed} \ \wedge \ \#A_{ir} = \#B_{ir} \ \wedge$$
$$(\#A^q_{er} - 1) = \#B^q_{er} \ \wedge \ \neg treeLocked \ \wedge \ last(A) = x \ \wedge \ last(A^q_{ed}) = x \ \wedge$$
$$\neg isRaReq \ \wedge \ \neg isIdReq \ \wedge \ \neg isEdReq \ \wedge \ \neg isIrReq \ \wedge \ isErReq$$

$$Q_{16} \stackrel{\text{def}}{=} \#A^q_{ra} = \#B^q_{ra} \ \wedge \ \#A_{id} = \#B_{id} = \#C_{id} \ \wedge \ \#A^q_{ed} = \#B^q_{ed} \ \wedge \ \#A_{ir} = \#B_{ir} \ \wedge$$
$$\#A^q_{er} = \#B^q_{er} \ \wedge \ \neg treeLocked \ \wedge \ last(A) = x \ \wedge$$
$$last(A^q_{er}) = x \ \wedge \ last(B^q_{er}) = y \ \wedge \ isUniquePID(last(B^q_{er}).spid)$$
$$\neg isRaReq \ \wedge \ \neg isIdReq \ \wedge \ \neg isEdReq \ \wedge \ \neg isIrReq \ \wedge \ isErReq$$

$$Q_{t^i_{qh}} \stackrel{\text{def}}{=} false$$

We check the following implications to prove that the above assertion network is an A-C-inductive assertion network w.r.t. assumption A^i_{qh}, commitment C^i_{qh}, and channels A, C, E,A^q_{ra}, B^q_{ra}, A_{id}, B_{id}, A^q_{ed}, B^q_{ed}, A_{ir}, B_{ir}, A^q_{er}, and B^q_{er}.

- $\models Q_{s^i_{qh}} \rightarrow C^i_{qh}$ follows from the above definitions.
- $\models Q_{s^i_{qh}} \ \wedge \ A^i_{qh} \rightarrow Q_{l_1} \circ init$. In this internal transition, function *init* does unset boolean variables *reeLocked*, *isRaReq*, *isIdReq*, *isIrReq*, *isEdReq*, and *isErReq*. Hence, this verification holds.
- $\models Q_{l_1} \ \wedge \ A^i_{qh} \rightarrow ((A^i_{qh} \rightarrow Q_{l_2}) \ \wedge \ C^i_{qh} \circ (f_1 \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x, \ h \mapsto v, \ \sigma(h).(A, v))$ for arbitrary v. In this input transition, a communication through channel A just took place. Function g assigns the last received value from channel A to x. The first implication of A^i_{qh} satisfies $isUniquePID(last(A).spid)$ predicate because $\#A > 0$. Function f_1 checks the variable x to find the request type and assigns boolean variables *isRaReq*, *isIdReq*, *isIrReq*, *isEdReq*, and *isErReq*, accordingly. Thus, this verification holds.
- $\models Q_{l_2} \ \wedge \ isRaReq \ \wedge \ A^i_{qh} \rightarrow ((A^i_{qh} \rightarrow Q_{l_3}) \ \wedge \ C^i_{qh}) \circ (g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A^q_{ra}, \sigma(x)))$. In this output transition, program I_{qh} sends x through channel A^q_{ra} toward program I^q_{ra}. From the transition's condition we have $isRaReq$. C^i_{qh} holds because $\#A^q_{ra} > 0$ and $\sigma \models isUniquePID(x.spid)$. Hence, this verification holds.
- $\models Q_{l_3} \wedge A^i_{qh} \rightarrow ((A^i_{qh} \rightarrow Q_{l_4}) \wedge C^i_{qh}) \circ (g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : y, h \mapsto v, \sigma(h).(B^q_{ra}, v))$ for arbitrary v. In this input transition, a communication through channel B^q_{ra} just took place and function g assigns the last received value to y. Because $\#A^q_{ra} = \#B^q_{ra} > 0$, the second implication of A^i_{qh} satisfies $isUniquePID(last(B^q_{ra}).spid)$. Thus, this verification holds.
- $\models Q_{l_4} \ \wedge \ A^i_{qh} \rightarrow ((A^i_{qh} \rightarrow Q_{l_1}) \ \wedge \ C^i_{qh}) \circ (f_4 \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(C, \sigma(y)))$. In this output transition, program I_{qh} just sends out variable y through channel C. Furthermore, function f_4 does unset boolean variables *isRaReq*, *isIdReq*, *isIrReq*, *isEdReq*, and *isErReq*. C^i_{qh} holds because $\#C > 0$, and $\sigma \models isUniquePID(last(C).cap)$. Hence, this verification holds.

- $\models Q_{l_2} \wedge isIdReq \wedge A^i_{qh} \rightarrow Q_{l_{i,5}} \circ f_1$. In this internal transition, function f_1 locks tree and set the variable *lockedTree*. Furthermore, the condition of the transition satisfies that *isIrReg* is set. Thus, this verification holds.

- $\models Q_{l_5} \wedge isidReq \wedge A^i_{qh} \rightarrow ((A^i_{qh} \rightarrow Q_{l_6}) \wedge C^i_{qh}) \circ (g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A_{id}, \sigma(x)))$. In this output transition, program I_{qh} sends x through channel A_{id} toward program I_{id}. C^i_{qh} holds because $\#A_{id} > 0$ and from Q_{l_5} we have $isUniquePID(x.spid)$. Hence, this verification holds.

- $\models Q_{l_6} \wedge A^i_{qh} \rightarrow ((A^i_{qh} \rightarrow Q_{l_7}) \wedge C^i_{qh}) \circ (g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : y, h \mapsto v, \sigma(h).(B_{id}, v))$ for arbitrary v. In this input transition, a communication through channel B_{id} just took place and function g assigns the last received value to y. Because $\#B_{id} > 0$, the second implication of A^i_{qh} satisfies $isValidCap(last(B_{id}).cap)$. Thus, this verification holds.

- $\models Q_{l_7} \wedge A^i_{qh} \rightarrow ((A^i_{qh} \rightarrow Q_{l_8}) \wedge C^i_{qh}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(E, \sigma(y)))$. In this output transition, program I_{qh} just sends out variable y through channel E. C^i_{qh} holds because $\#E > 0$ and $\sigma \models valid(last(C).cap)$. Hence, this verification holds.

- $\models Q_{l_8} \wedge A^i_{qh} \rightarrow ((A^i_{qh} \rightarrow Q_{l_9}) \wedge C^i_{qh}) \circ (g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : z, h \mapsto v, \sigma(h).(C_{id}, v))$ for arbitrary v. In this input transition, a communication through channel C_{id} just took place and function g assigns the last received value to z. Because $\#C_{id} > 0$, the second implication of A^i_{qh} satisfies $isIdConfRes(last(C_{id}))$. Thus, this verification holds.

- $\models Q_{l_9} \wedge A^i_{qh} \rightarrow ((A^i_{qh} \rightarrow Q_{l_1}) \wedge C^i_{qh}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(E, \sigma(z)))$. In this output transition, program I_{qh} just sends out variable z through channel E. Because $\#E > 0 \wedge isIrReq$, then C^i_{qh} holds. Furthermore, function f_4 does unset boolean variables *reeLocked*, *isRaReq*, *isIdReq*, *isIrReq*, *isEdReq*, and *isErReq*. Hence, this verification holds.

- $\models Q_{l_2} \wedge isEdReq \wedge A^i_{qh} \rightarrow ((A^i_{qh} \rightarrow Q_{l_{10}}) \wedge C^i_{qh}) \circ (g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A^q_{ed}, \sigma(x)))$. In this output transition, program I_{qh} sends x through channel A^q_{ed} toward program I^q_{ed}. From the transition's condition we have $isEdReq$. C^i_{qh} holds because $\#A^q_{ed} > 0$ and $\sigma \models isUniquePID(x.spid)$. Hence, this verification holds.

- $\models Q_{l_{10}} \wedge A^i_{qh} \rightarrow ((A^i_{qh} \rightarrow Q_{l_{11}}) \wedge C^i_{qh}) \circ (g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : y,\ h \mapsto v,\ \sigma(h).(B^q_{ed}, v))$ for arbitrary v. In this input transition, a communication through channel B^q_{ed} just took place and function g assigns the last received value to y. the implication of A^i_{qh} satisfies $isUniquePID(last(B^q_{ed}).spid)$ because $\#A^q_{ed} = \#B^q_{ed} > 0$. Thus, this verification holds.

- $\models Q_{l_{11}} \wedge A^i_{qh} \rightarrow ((A^i_{qh} \rightarrow Q_{l_1}) \wedge C^i_{qh}) \circ (f_4 \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(C, \sigma(y)))$. In this output transition, program I_{qh} just sends out variable y through channel C. Furthermore, function f_4 does unset boolean variables *isRaReq*, *isIdReq*, *isIrReq*, *isEdReq*, and *isErReq*. C^i_{qh} holds because $\#C > 0$, and $\sigma \models isUniquePID(last(C).cap)$. Hence, this verification holds.

- $\models Q_{l_2} \wedge isIrReq \wedge A^i_{qh} \rightarrow Q_{l_{i,12}} \circ f_1$. In this internal transition, function f_1 locks tree and set the variable *lockedTree*. Furthermore, the condition of the transition satisfies that *isIrReq* is unset. Thus, this verification holds.
- $\models Q_{l_{12}} \wedge isidReq \wedge A^i_{qh} \rightarrow ((A^i_{qh} \rightarrow Q_{l_{13}}) \wedge C^i_{qh}) \circ (g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A_{ir}, \sigma(x)))$. In this output transition, program I_{qh} sends x through channel A_{ir} toward program I_{ir}. C^i_{qh} holds because $\#A_{ir} > 0$ and $\sigma \models isUniquePID(x.spid)$. Hence, this verification holds.
- $\models Q_{l_{13}} \wedge A^i_{qh} \rightarrow ((A^i_{qh} \rightarrow Q_{l_{14}}) \wedge C^i_{qh}) \circ (g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : y,\ h \mapsto v,\ \sigma(h).(B_{ir}, v))$ for arbitrary v. In this input transition, a communication through channel B_{ir} just took place and function g assigns the last received value to y. Because $\#B_{ir} > 0$, the second implication of A^i_{qh} satisfies $isIrConfRes(last(B_{ir}).cap)$. Thus, this verification holds.
- $\models Q_{l_{14}} \wedge A^i_{qh} \rightarrow ((A^i_{qh} \rightarrow Q_{l_1}) \wedge C^i_{qh}) \circ (f_4 \circ f_3 \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(E, \sigma(y)))$. In this output transition, program I_{qh} just sends out variable y through channel E. C^i_{qh} holds because $\#E > 0$ and $\sigma \models isIrConfRes(last(E).cap)$. Function f_3 unlocks the tree and function f_4 does unset boolean variables *isRaReq*, *isIdReq*, *isIrReq*, *isEdReq*, and *isErReq*. Hence, this verification holds.
- $\models Q_{l_2} \wedge isErReq \wedge A^i_{qh} \rightarrow ((A^i_{qh} \rightarrow Q_{l_{15}}) \wedge C^i_{qh}) \circ (g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A^q_{er}, \sigma(x)))$. In this output transition, program I_{qh} sends x through channel A^q_{er} toward program I^q_{er}. From the transition's condition we have $isErReq$. C^i_{qh} holds because $\#A^q_{er} > 0$ and $\sigma \models isUniquePID(x.spid)$. Hence, this verification holds.
- $\models Q_{l_{15}} \wedge A^i_{qh} \rightarrow ((A^i_{qh} \rightarrow Q_{l_{16}}) \wedge C^i_{qh}) \circ (g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : y,\ h \mapsto v,\ \sigma(h).(B^q_{er}, v))$ for arbitrary v. In this input transition, a communication through channel B^q_{ed} just took place and function g assigns the last received value to y. A^i_{qh} satisfies $isUniquePID(last(B^q_{er}).spid)$ Because $\#A^q_{er} = \#B^q_{er} > 0$. Thus, this verification holds.
- $\models Q_{l_{16}} \wedge A^i_{qh} \rightarrow ((A^i_{qh} \rightarrow Q_{l_1}) \wedge C^i_{qh}) \circ (f_4 \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(C, \sigma(y)))$. In this output transition, program I_{qh} just sends out variable y through channel C. Furthermore, function f_4 does unset boolean variables *isRaReq*, *isIdReq*, *isIrReq*, *isEdReq*, and *isErReq*. C^i_{qh} holds because $\#C > 0$, and $\sigma \models isUniquePID(last(C).cap)$. Hence, this verification holds.

6.2.2.2 Response Handling

We model the response handler by the program I_{sh}. It cooperates with three programs to handle responses, including I^s_{ra} (resource-allocation response handler), I^s_{ed} (the external-delegation response handler), and I^s_{er} (the external-revocation response handler). In addition, I_{sh} directly forwards all the responses from the request handler to O. Program I_{sh} assumes that all received responses from the resource controllers are valid. Furthermore, it commits to forwarding received responses to the corresponding programs and forwarding programs' responses to O directly. Figure 20 depicts the state diagram of program I_{sh}.

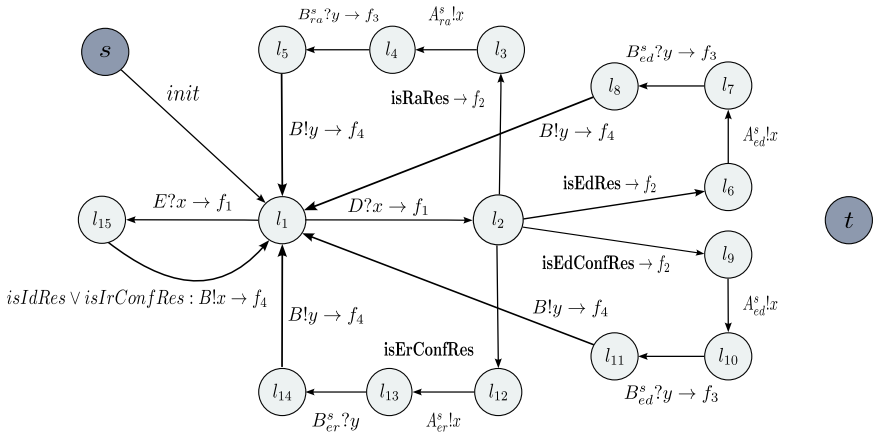


Figure 20: Response-Handler Program of the Intermediate Controller.

Program I_{sh} receives responses from resource controllers via channel D. It uses four predicates to find out the type of a responses and forward it to the corresponding module. Then, the handler receives the response and forwards it to the operating system via channel B. In addition, it receives the responses from the request handler through channel E and forward them via channel B The conditions and functions of I_{sh} are defined as follow:

$$
\begin{aligned}
init(\sigma) = \ & (\sigma : rootPtr, treeLocked, \\
& isRaRes, isEdRes, isEdConfRes, isErConfRes, isIdfRes, isIrConfRes \\
& \mapsto getRoot(\sigma(icTree)), false, false, false, false, false\ false), \\
f_1(\sigma) = \ & (\sigma : isRaRes, isEdRes, isEdConfRes, isErConfRes, isIdfRes, \\
& isIrConfRes \mapsto isRaResCheck(\sigma(x)), isEdResCheck(\sigma(x)), \\
& isEdConfResCheck(\sigma(x)), isErConfResCheck(\sigma(x)), \\
& isIdfResCheck(\sigma(x)), isIrConfRes(\sigma(x))), \\
f_2(\sigma) = \ & (\sigma : treeLocked \mapsto lockTree(\sigma(rootPtr))), \\
f_3(\sigma) = \ & (\sigma : treeLocked \mapsto unlockTree(\sigma(rootPtr))), \\
f_4(\sigma) = \ & (\sigma : isRaRes, isEdRes, isEdConfRes, isErConfRes, isIdfRes, \\
& isIrConfRes \mapsto false, false, false, false, false, false)
\end{aligned}
$$

The A-C formula for process I_{sh} is as follows:

$$\vdash \langle A^i_{sh}\ C^i_{sh} \rangle\ \{\varphi^i_{sh}\}\ I_{sh}\ \{\psi^i_{sh}\}$$

where the formal definition of φ^i_{sh}, ψ^i_{sh} , A^i_{sh}, and C^i_{sh} are as follows:

$$\varphi^i_{sh} \stackrel{\text{def}}{=} \#B = \#D = \#E = 0\ \wedge\ \#A^s_{ra} = \#B^s_{ra} = 0\ \wedge\ \#A^s_{ed} = \#B^s_{ed} = 0 \wedge$$

$$\#A^s_{er} = \#B^s_{er} = 0 \ \wedge \ \neg treeLocked \ \wedge \ \neg isRaRes \ \wedge \ \neg isEdRes \wedge$$
$$\neg isEdConfRes \ \wedge \ \neg isIdfRes \ \wedge \ \neg isIrConfRes$$

$$\psi^i_{sh} \stackrel{\text{def}}{=} false$$

$$A^i_{sh} \stackrel{\text{def}}{=} ((\#D > 0 \wedge (isRaRes \vee isEdRes \vee isEdConfRes))$$
$$\rightarrow isValidCap(last(D).cap)) \wedge$$
$$((\#B^s_{ra} > 0) \rightarrow isValidCap(last(B^s_{ra}).cap)) \wedge$$
$$((\#B^s_{ed} > 0) \rightarrow isValidCap(last(B^s_{ed}).cap))$$
$$((\#B^s_{er} > 0) \rightarrow isErConfRes(last(B^s_{er}))) \wedge$$

$$C^i_{sh} \stackrel{\text{def}}{=} ((\#B > 0 \wedge (isRaRes \vee isEdRes \vee isEdConfRes \vee isIdfRes))$$
$$\rightarrow isValidCap(last(B).cap))) \wedge$$
$$((\#B > 0 \wedge isErConfRes) \rightarrow isErConfRes(last(B)))) \wedge$$
$$((\#A^s_{ra} > 0) \rightarrow isRaRes(last(A^s_{ra})) \ \wedge \ isValidCap(last(A^s_{ra}).cap)) \wedge$$
$$((\#A^s_{ed} > 0) \rightarrow (isEdRes(last(A^s_{ed})) \vee isEdConfRes(last(A^s_{ed})) \wedge$$
$$isValidCap(last(A^s_{ed}).cap))$$

The assertion network for I_{sh} is as follows:

$$Q_{s^i_{sh}} \stackrel{\text{def}}{=} \#B = \#D = \#E = 0 \ \wedge \ \#A^s_{ra} = \#B^s_{ra} = 0 \ \wedge \ \#A^s_{ed} = \#B^s_{ed} = 0 \wedge$$
$$\#A^s_{er} = \#B^s_{er} = 0 \ \wedge \ \neg treeLocked \ \wedge \ \neg isRaRes \ \wedge \ \neg isEdRes \wedge$$
$$\neg isEdConfRes \ \wedge \ \neg isErConfRes \ \wedge \ \neg isIdfRes \ \wedge \ \neg isIrConfRes$$

$$Q_2 \stackrel{\text{def}}{=} \#A^s_{ra} = \#B^s_{ra} = 0 \ \wedge \ \#A^s_{ed} = \#B^s_{ed} = 0 \ \wedge \ \#A^s_{er} = \#B^s_{er} = 0 \ \wedge \ \neg treeLocked \wedge$$
$$last(D) = x$$

$$Q_3 \stackrel{\text{def}}{=} \#A^s_{ra} = \#B^s_{ra} = 0 \ \wedge \ \#A^s_{ed} = \#B^s_{ed} = 0 \ \wedge \ \#A^s_{er} = \#B^s_{er} = 0 \ \wedge \ last(D) = x$$
$$treeLocked \ \wedge \ isRaRes \ \wedge \ \neg isEdRes \ \wedge \ \neg isEdConfRes \wedge$$
$$\neg isErConfRes \ \wedge \ negisIdfRes \ \wedge \ \neg isIrConfRes \ \wedge \ last(D) = x \wedge$$
$$isValidCap(last(D))$$

$$Q_4 \stackrel{\text{def}}{=} \#A^s_{ra} - 1 = \#B^s_{ra} = 0 \ \wedge \ \#A^s_{ed} = \#B^s_{ed} = 0 \ \wedge \ \#A^s_{er} = \#B^s_{er} = 0 \ \wedge \ last(D) = x$$
$$treeLocked \ \wedge \ isRaRes \ \wedge \ \neg isEdRes \ \wedge \ \neg isEdConfRes \ \wedge \ \neg isErConfRes \wedge$$
$$\neg isIdfRes \ \wedge \ \neg isIrConfRes \ \wedge \ last(D) = x \ \wedge \ last(A^s_{ra}) = x \wedge$$
$$isValidCap(last(A^s_{ra}))$$

$$Q_5 \stackrel{\text{def}}{=} \#A^s_{ra} - 1 = \#B^s_{ra} = 0 \ \wedge \ \#A^s_{ed} = \#B^s_{ed} = 0 \ \wedge \ \#A^s_{er} = \#B^s_{er} = 0 \ \wedge \ last(D) = x$$
$$\neg treeLocked \ \wedge \ isRaRes \ \wedge \ \neg isEdRes \ \wedge \ \neg isEdConfRes \wedge$$
$$\neg isErConfRes \ \wedge \ \neg isIdfRes \ \wedge \ \neg isIrConfRes \ \wedge \ last(D) = x \wedge$$
$$last(A^s_{ra}) = x \ \wedge \ last(B^s_{ra}) = y \ \wedge \ isValidCap(last(B^s_{ra}))$$

$$Q_6 \stackrel{\text{def}}{=} \#A^s_{ra} = \#B^s_{ra} = 0 \ \wedge \ \#A^s_{ed} = \#B^s_{ed} = 0 \ \wedge \ \#A^s_{er} = \#B^s_{er} = 0 \ \wedge \ last(D) = x$$
$$treeLocked \ \wedge \ \neg isRaRes \ \wedge \ isEdRes \ \wedge \ \neg isEdConfRes \wedge$$

$$\neg isErConfRes \wedge negisIdfRes \wedge \neg isIrConfRes \wedge last(D) = x \wedge isValidCap(last(D))$$

$$Q_7 \stackrel{\text{def}}{=} \#A^s_{ra} = \#B^s_{ra} = 0 \wedge \#A^s_{ed} - 1 = \#B^s_{ed} = 0 \wedge \#A^s_{er} = \#B^s_{er} = 0 \wedge last(D) = x \; treeLocked \wedge \neg isRaRes \wedge isEdRes \wedge \neg isEdConfRes \wedge \neg isErConfRes \wedge \neg isIdfRes \wedge \neg isIrConfRes \wedge last(D) = x \wedge last(A^s_{ra}) = x \wedge isValidCap(last(A^s_{ed}))$$

$$Q_8 \stackrel{\text{def}}{=} \#A^s_{ra} - 1 = \#B^s_{ra} = 0 \wedge \#A^s_{ed} = \#B^s_{ed} = 0 \wedge \#A^s_{er} = \#B^s_{er} = 0 \wedge last(D) = x \; \neg treeLocked \wedge \neg isRaRes \wedge isEdRes \wedge \neg isEdConfRes \wedge \neg isErConfRes \wedge \neg isIdfRes \wedge \neg isIrConfRes \wedge last(D) = x \wedge last(A^s_{ed}) = x \wedge last(B^s_{ed}) = y \wedge isValidCap(last(B^s_{ed}))$$

$$Q_9 \stackrel{\text{def}}{=} \#A^s_{ra} = \#B^s_{ra} = 0 \wedge \#A^s_{ed} = \#B^s_{ed} = 0 \wedge \#A^s_{er} = \#B^s_{er} = 0 \wedge last(D) = x \; treeLocked \wedge \neg isRaRes \wedge \neg isEdRes \wedge isEdConfRes \wedge \neg isErConfRes \wedge negisIdfRes \wedge \neg isIrConfRes \wedge last(D) = x \wedge isValidCap(last(D))$$

$$Q_{10} \stackrel{\text{def}}{=} \#A^s_{ra} = \#B^s_{ra} = 0 \wedge \#A^s_{ed} - 1 = \#B^s_{ed} = 0 \wedge \#A^s_{er} = \#B^s_{er} = 0 \wedge last(D) = x \; treeLocked \wedge \neg isRaRes \wedge \neg isEdRes \wedge isEdConfRes \wedge \neg isErConfRes \wedge \neg isIdfRes \wedge \neg isIrConfRes \wedge last(D) = x \wedge last(A^s_{ra}) = x \wedge isValidCap(last(A^s_{ed}))$$

$$Q_{11} \stackrel{\text{def}}{=} \#A^s_{ra} - 1 = \#B^s_{ra} = 0 \wedge \#A^s_{ed} = \#B^s_{ed} = 0 \wedge \#A^s_{er} = \#B^s_{er} = 0 \wedge last(D) = x \; \neg treeLocked \wedge \neg isRaRes \wedge \neg isEdRes \wedge isEdConfRes \wedge \neg isErConfRes \wedge \neg isIdfRes \wedge \neg isIrConfRes \wedge last(D) = x \wedge last(A^s_{ed}) = x \wedge last(B^s_{ed}) = y \wedge isValidCap(last(B^s_{ed}))$$

$$Q_{12} \stackrel{\text{def}}{=} \#A^s_{ra} = \#B^s_{ra} = 0 \wedge \#A^s_{ed} = \#B^s_{ed} = 0 \wedge \#A^s_{er} = \#B^s_{er} = 0 \wedge last(D) = x \; treeLocked \wedge \neg isRaRes \wedge \neg isEdRes \wedge \neg isEdConfRes \wedge isErConfRes \wedge negisIdfRes \wedge \neg isIrConfRes \wedge last(D) = x$$

$$Q_{13} \stackrel{\text{def}}{=} \#A^s_{ra} = \#B^s_{ra} = 0 \wedge \#A^s_{ed} = \#B^s_{ed} = 0 \wedge \#A^s_{er} - 1 = \#B^s_{er} = 0 \wedge last(D) = x \; treeLocked \wedge \neg isRaRes \wedge \neg isEdRes \wedge \neg isEdConfRes \wedge isErConfRes \wedge \neg isIdfRes \wedge \neg isIrConfRes \wedge last(D) = x \wedge last(A^s_{ra}) = x$$

$$Q_{14} \stackrel{\text{def}}{=} \#A^s_{ra} - 1 = \#B^s_{ra} = 0 \wedge \#A^s_{ed} = \#B^s_{ed} = 0 \wedge \#A^s_{er} = \#B^s_{er} = 0 \wedge last(D) = x \; \neg treeLocked \wedge \neg isRaRes \wedge \neg isEdRes \wedge \neg isEdConfRes \wedge isErConfRes \wedge \neg isIdfRes \wedge \neg isIrConfRes \wedge last(D) = x \wedge last(A^s_{er}) = x \wedge last(B^s_{er}) = y$$

$$Q_{15} \stackrel{\text{def}}{=} \#A^s_{ra} = \#B^s_{ra} = 0 \wedge \#A^s_{ed} = \#B^s_{ed} = 0 \wedge \#A^s_{er} = \#B^s_{er} = 0 \wedge \neg treeLocked$$

$$\wedge\ \neg isRaRes\ \wedge\ \neg isEdRes\ \wedge\ \neg isEdConfRes\ \wedge\ isErConfRes \wedge$$
$$(isIdfRes \vee isIrConfRes)\ \wedge\ last(E) = x$$

Now, we check the validity of the hypothesis in Rule 1. Program I_{qh} receives requests from channel A and processes them in a FIFO order. Because I_{qh} assumes each request contains a unique process ID and commits to forwarding the request to the right program, it satisfies the assumption of programs I^q_{ra} (A^q_{ra}), I_{id} (A_{id}), I^q_{ed} (A^q_{ed}), I_{ir} (A_{ir}), and I^q_{er} (A^q_{er}). I_{sh} processes received responses from channel D. Because each response contains a valid capability and I_{sh} commits forwarding it to the right program. Furthermore, I_{sh} receives valid responses from programs I^s_{ra}, I^s_{ed}, and I^s_{er}, and forward them via channel B.

6.3 Parallel Composition

The instantiated access-control system (denoted by program S) comprises programs R, I, and O, running in parallel ($S \stackrel{\text{def}}{=} R \parallel I \parallel O$). Hence, We apply the parallel composition rule to acquire the instantiated system's A-C formula as the following:

$$\vdash \langle A^s,\ C^s \rangle :\ \{\varphi^s\}\ S\ \{\psi^s\}$$

Program O commits to program I that each process uses its PID when sending a request, and the PID is unique. Furthermore, program O commits to forwarding responses to their corresponding processes directly. In addition, the commitments of programs R and I comprise their modules' commitments. Therefore, the above A-C formula proves Lemmas 1 to 5 for the instantiated system.

6.4 Proof

In this section, we proof the above lemmas for the MDC design. We proof the lemmas using the rely-guarantee technique too. In addition, we use the proofs of those lemmas as the building blocks in proofs of the lemmas for the MDC design.

To proof the lemmas, we model an operating system, an intermediate controller, and a resource controller by programs $O \stackrel{\text{def}}{=} (L_o, T_o, s_o, t_o)$, $I \stackrel{\text{def}}{=} (L_i, T_i, s_i, t_i)$, and $R \stackrel{\text{def}}{=} (L_r, T_r, s_r, t_r)$, respectively. Program I is defined as parallel execution of the programs of the modules in the intermediate controller as following:

$$I \stackrel{\text{def}}{=} I_{H_q} \parallel I_{H_s} \parallel I_{ra} \parallel I_{ld} \parallel I_{rd} \parallel I^d_{rd} \parallel I_{rr}$$

Program R is defined as parallel execution of the programs of the modules in the resource controller as following:

$$R \stackrel{\text{def}}{=} R_{h_{qs}} \parallel R_{ra} \parallel R_{rd} \parallel R_{rr}$$

Now, we proof the lemmas regarding these programs.

6.4.1 First Lemma: Resource Allocation

First lemma indicates that any resource-allocation operation creates a valid p-cap. We formally define the lemma and proof it.

Lemma 6. *Given a process with unique ID in a process node, a intermediate controller in the same node, and a resource controller in a resource node, the process will get a valid p-cap by sending a resource-allocation request.*

Proof. We use Assumption-Commitment technique to prove the lemma.

Program I_{qh} receives a request from process P_{ra} via channel A and finds out the request is a resource-allocation one. Then, I_{qh} forwards the request to program I^q_{ra}, receives the response from it, and forwards the response toward program R through channel C.

The A-C formula for program I_{qh} is as follows:

$$\vdash \langle Ass_{qh},\ C_{qh}\rangle\ \{\varphi_{qh}\}\ I_{qh}\ \{\psi_{qh}\}$$

where φ_{qh}, ψ_{qh} , Ass_{qh}, and C_{qh} are formalised as follows:

$$\begin{aligned}
\varphi_{qh} &\stackrel{\text{def}}{=} \#A = \#C = 0\ \wedge\ \#A^q_{ra} = \#B^q_{ra} = 0\\
\psi_{qh} &\stackrel{\text{def}}{=} false\\
Ass_{qh} &\stackrel{\text{def}}{=} (\#A > 0 \rightarrow isUniquePID(last(A).spid)) \wedge\\
&\quad (\#B^q_{ra} > 0 \rightarrow\\
&\qquad isRaReq(last(B^q_{ra}))\ \wedge\ isUniquePID(last(B^q_{ra}).spid))\\
C_{qh} &\stackrel{\text{def}}{=} (\#B > 0 \rightarrow isUniquePID(last(B).spid)) \wedge\\
&\quad (\#A^q_{ra} > 0 \rightarrow\\
&\qquad isRaReq(last(A^q_{ra}))\ \wedge\ isUniquePID(last(A^q_{ra}).spid))
\end{aligned}$$

wherein N_a, N_b, and 0 are logical variables.

The assertion network for I_{qh} is as follows:

$$\begin{aligned}
Q_s &\stackrel{\text{def}}{=} \#A = \#C = 0\ \wedge\ \#A^q_{ra} = \#B^q_{ra} = 0\\
Q_{l_1} &\stackrel{\text{def}}{=} \#A^q_{ra} = \#B^q_{ra}\\
Q_{l_2} &\stackrel{\text{def}}{=} \#A^q_{ra} = \#B^q_{ra}\ \wedge\ last(A) = x\\
Q_{l_3} &\stackrel{\text{def}}{=} (\#A^q_{ra} - 1) = \#B^q_{ra}\ \wedge\ last(A) = x \wedge\\
&\qquad last(A^q_{ra}) = x\\
Q_{l_4} &\stackrel{\text{def}}{=} \#A^q_{ra} = \#B^q_{ra}\ \wedge\ last(A) = x \wedge\\
&\qquad last(A^q_{ra}) = x\ \wedge\ last(B^q_{ra}) = y\\
Q_t &\stackrel{\text{def}}{=} false
\end{aligned}$$

We check the following verifications to prove that above assertion network is an A-C-inductive assertion network w.r.t. assumption Ass_{qh}, commitment C_{qh}, and channels A, B, A^q_{ra}, and B^q_{ra}.

- $\models Q_s \rightarrow C_{qh}$ follows from the above definition.
- $\models Q_s \wedge Ass_{qh} \rightarrow Q_{l_1} \circ init$. In this internal transition, function *init* does not change the state of the program. Hence, this verification holds.
- $\models Q_{l_1} \wedge Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_2}) \wedge C_{qh}) \circ (f_1 \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x,\ h \mapsto v,\ \sigma(h).(A, v))$ for arbitrary value $v \in MSG$. In this input transition, $\sigma' \models \#A > 0$ holds because just a communication through channel A took place. Function g assigns the received value to variable x. Since $\#A > 0$, the first implication of Ass_{qh} satisfies $isUniquePID(last(A).spid)$. Thus, this verification holds.
- $\models Q_{l_2} \wedge isRAReq(x) \wedge Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_3}) \wedge C_{qh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A^q_{ra}, \sigma(x)))$. In this output transition, the request in variable x is forwarded toward resource-allocation module through channel A^q_{ra} because $isRaReq(x)$ is evaluated to *true*. C_{qh} is satisfied because $\#A^q_{ra} > 0$, from the condition of the transition we have $isRaReq(last(A^q_{ra}))$, and from Q_{l_2} we have $isUniquePID(last(A^q_{ra}).spid)$. Thus, this verification holds.
- $\models Q_{l_3} \wedge Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_4}) \wedge C_{qh}) \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : y,\ h \mapsto v,\ \sigma(h).(B^q_{ra}, v))$ for arbitrary value $v \in MSG$. In this input transition, the program receives the response of program I_{ra} through channel B^q_{ra} and assign it to variable y via function g. Since $\#B^q_{ra} > 0$, the first implication of Ass_{qh} implies $isRaReq(last(B^q_{ra}))$ and $isUniquePID(last(B^q_{ra}).spid)$. Thus, this verification holds.

  $\models Q_{l_4} \wedge Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_1}) \wedge C_{qh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B, \sigma(y)))$. In this output transition, the program sends the request in variable y through channel B. C_{qh} holds because from Q_{l_3} we have $isRaReq(y)$ and $isUniquePID(y.spid)$. Hence, this verification holds.

Finally, the post-condition of program I_{qh} is satisfied because $Q_t \rightarrow \psi_{qh}$.

Program R_h receives a request from program I via channel A and finds out the request is resource-allocation one. Then, R_h forwards the request to program R_{ra}, receives the response from it, and forwards the response toward program I through channel B.

The A-C formula for process R_h is as follows:

$$\vdash \langle Ass_h,\ C_h \rangle\ \{\varphi_h\}\ I_h\ \{\psi_h\}$$

where φ_h, ψ_h , Ass_h, and C_h are formalised as follows:

$$\begin{array}{lll}
\varphi_h & \stackrel{\text{def}}{=} & \#A \geq 0 \ \wedge\ \#B \geq 0 \ \wedge\ \#A_{ra} = \#B_{ra} \\
\psi_h & \stackrel{\text{def}}{=} & false \\
Ass_h & \stackrel{\text{def}}{=} & (\#A > 0 \rightarrow isUniquePID(last(A).spid)) \wedge \\
 & & (\#B_{ra} > 0 \rightarrow \\
 & & \quad isRaRes(last(B_{ra})) \ \wedge\ isValidCap(last(B_{ra}).cap)
\end{array}$$

$$C_h \quad \stackrel{\text{def}}{=} \quad (\#B > 0 \rightarrow isRaRes(last(B)) \ \wedge \ isValidCap(last(B).cap)) \wedge (\#A_{ra} > 0 \rightarrow isRaReq(last(A_{ra})) \ \wedge \ isUniquePID(last(A_{ra}).spid))$$

wherein 0 is a logical variable.

The assertion network for R_h is as follows:

$$Q_s \stackrel{\text{def}}{=} \#A = \#C = 0 \ \wedge \ \#A_{ra} = \#B_{ra} = 0$$

$$Q_{l_1} \stackrel{\text{def}}{=} \#A_{ra} = \#B_{ra}$$

$$Q_{l_2} \stackrel{\text{def}}{=} \#A_{ra} = \#B_{ra} \ \wedge \ last(A) = x$$

$$Q_{l_3} \stackrel{\text{def}}{=} (\#A_{ra} - 1) = \#B_{ra} \ \wedge \ last(A) = x \ \wedge \ last(A_{ra}) = x$$

$$Q_{l_4} \stackrel{\text{def}}{=} \#A^q_{ra} = \#B^q_{ra} \ \wedge \ last(A) = x \ \wedge \ last(A_{ra}) = x \wedge last(B_{ra}) = y$$

$$Q_t \stackrel{\text{def}}{=} false$$

We check the following verifications to prove that above assertion network is an A-C-inductive assertion network w.r.t. assumption Ass_h, commitment C_h, and channels A, B, A_{ra}, and B_{ra}.

- $\models Q_s \rightarrow C_h$ follows from the above definition.
- $\models Q_s \ \wedge \ Ass_h \rightarrow Q_{l_1} \ \circ \ init$. In this internal transition, function *init* does not change the state of the program. Hence, this verification holds.
- $\models Q_{l_1} \wedge Ass_h \rightarrow ((Ass_h \rightarrow Q_{l_2}) \wedge C_h) \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x, h \mapsto v, \sigma(h).(M, v))$ for arbitrary value $v \in MSG$. In this input transition, the program receives a message through channel M and function g stores it in variable x. Based on Ass_h, we have $isUniquePID(last(x).spid))$. Thus, this verification holds.
- $\models Q_{l_2} \ \wedge \ isRAReq(x) \ \wedge \ Ass_h \rightarrow ((Ass_h \rightarrow Q_{l_3}) \ \wedge \ C_h))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A_{ra}, \sigma(x)))$. In this output transition, the request in variable x is forwarded toward resource-allocation module through channel $\#A_{ra}$ because $isRAReq(x)$ is evaluated to *true*. C_h is satisfied because $\#A_{ra} > 0$, from the condition of the transition we have $isRaReq(last(A_{ra}))$, and from Q_{l_2} we have $isUniquePID(last(A_{ra}).spid)$. Thus, this verification holds.

  $\models Q_{l_3} \wedge Ass_h \rightarrow ((Ass_h \rightarrow Q_{l_4}) \wedge C_h))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B_{ra}\sigma(y)))$. In this input transition, the program receives the resource-allocation response in variable y through channel B_{ra}. Hence, this verification holds.

  $\models Q_{l_4} \wedge Ass_h \rightarrow ((Ass_h \rightarrow Q_{l_1}) \wedge C_h))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B, \sigma(y)))$. In this output transition, the program sends the response in variable y through channel B. C_h holds because from Ass_h we have $isRaRes(y)$ and $isUniquePID(y.spid)$. Hence, this verification holds.

Finally, the post-condition of program R_h is satisfied because $Q_t \rightarrow \psi_h$.

Program I_{sh} receives a response from program R via channel D and finds out the response is a resource-allocation response. Then, I_{sh} forwards the response to I^s_{ra} module, receives the response from the module, and forwards the response toward program O via channel B.

The A-C formula for program I_{sh} is as follows:

$$\vdash \langle Ass_{sh},\ C_{sh} \rangle\ \{\varphi_{sh}\}\ I_{sh}\ \{\psi_{sh}\}$$

where φ_{sh}, ψ_{sh} , Ass_{sh}, and C_{sh} are formalised as follows:

$$\begin{aligned}
\varphi_{sh} &\stackrel{\text{def}}{=} \#C = 0\ \wedge\ \#D = N_d\ \wedge\ \#A^s_{ra} = \#B^s_{ra} = 0\ \wedge\ \neg hasTreeToken \\
\psi_{sh} &\stackrel{\text{def}}{=} false \\
Ass_{sh} &\stackrel{\text{def}}{=} (\#C > 0\ \wedge\ isRaRes(last(C)) \rightarrow isValidCap(last(C).cap)) \wedge \\
&\quad (\#B^s_{ra} > 0 \rightarrow \\
&\quad\quad isRaRes(last(B^s_{ra}))\ \wedge\ isValidCap(last(B^s_{ra}).cap)) \\
C_{sh} &\stackrel{\text{def}}{=} (\#D > N_d \rightarrow \\
&\quad\quad isRaRes(last(D))\ \wedge\ isValidCap(last(D).cap)) \wedge \\
&\quad (\#A^s_{ra} > 0 \rightarrow \\
&\quad\quad isRaRes(last(A^s_{ra}))\ \wedge\ isValidCap(last(A^s_{ra}).cap))
\end{aligned}$$

wherein 0, N_d, and 0 are logical variables.

The assertion network for I_{sh} is as follows:

$$\begin{aligned}
Q_s &\stackrel{\text{def}}{=} \#B = \#D = 0\ \wedge\ \#A^s_{ra} = \#B^s_{ra} = 0\ \wedge\ \neg hasTreeToken \\
Q_{l_1} &\stackrel{\text{def}}{=} \#A^s_{ra} = \#B^s_{ra}\ \wedge\ \neg hasTreeToken \\
Q_{l_2} &\stackrel{\text{def}}{=} \#A^s_{ra} = \#B^s_{ra}\ \wedge\ last(C) = x\ \wedge\ \neg hasTreeToken \\
Q_{l_3} &\stackrel{\text{def}}{=} \#A^s_{ra} = \#B^s_{ra}\ \wedge\ last(C) = x\ \wedge\ hasTreeToken \\
&\quad\ isRaRes(x)\ \wedge\ isValidCap(x.cap) \\
Q_{l_4} &\stackrel{\text{def}}{=} (\#A^s_{ra} - 1) = \#B^s_{ra}\ \wedge\ last(C) = x \wedge \\
&\quad\ last(A^s_{ra}) = x\ \wedge\ hasTreeToken \\
Q_{l_5} &\stackrel{\text{def}}{=} \#A^s_{ra} = \#B^s_{ra}\ \wedge\ last(C) = x\ \wedge\ last(A^s_{ra}) = x \wedge \\
&\quad\ last(B^s_{ra}) = y\ \wedge\ hasTreeToken\ \wedge\ isRaRes(y)\ \wedge\ isValidCap(y.cap) \\
Q_t &\stackrel{\text{def}}{=} false
\end{aligned}$$

We check the following verifications to prove that above assertion network is an A-C-inductive assertion network w.r.t. assumption Ass_{sh}, commitment C_{sh}, and channels B, D, A^s_{ra}, and B^s_{ra}.

- $\models Q_s \rightarrow C_{sh}$ follows from the above definition.

- $\models Q_s \wedge Ass_{sh} \rightarrow Q_{l_1} \circ init$. In this internal transition, function *init* does not change the state of the program. Hence, this verification holds.
- $\models Q_{l_1} \wedge Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_2}) \wedge C_{sh}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x,\ h \mapsto v,\ \sigma(h).(M, v))$ for arbitrary value $v \in MSG$. In this input transition, just a communication through channel C took place. Function g assigns the received value to variable x, hence $last(C) = x$. Thus, this verification holds.
- $\models Q_{l_2} \wedge isRaRes(x) \wedge Ass_{sh} \rightarrow Q_{l_3} \circ f_1$. In this internal transition, function f_1 gets the tree token. Since $\#C > 0$ and $isRaRes(x)$, from Ass_{sh} we have $isValidCap(x.cap)$). Thus, this verification holds.
- $\models Q_{l_3} \wedge Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_4}) \wedge C_{sh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A^s_{ra}, \sigma(x)))$. In this output transition, the response in variable x is forwarded toward resource-allocation module through channel A^s_{ra}. C_{qh} is satisfied because $\#A^s_{ra} > 0$ and from Q_{l_3} we have $isRaRes(last(A^s_{ra}))$ and $isValidCap(last(A^s_{ra}).cap)$. Thus, this verification holds.
- $\models Q_{l_4} \wedge Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_5}) \wedge C_{sh}) \circ g)$where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : y,\ h \mapsto v,\ \sigma(h).(B^s_{ra}, v))$ for arbitrary value $v \in MSG$. In this input transition, the program receives the response of program I_{ra} through channel B^s_{ra} and assign it to variable y via function g. Since $\#B^s_{ra} > 0$, the first implication of Ass_{sh} implies $isRaRes(last(B^s_{ra}))$ and $isValidCap(last(B^s_{ra}).cap)$. Thus, this verification holds.

  $\models Q_{l_5} \wedge Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_1}) \wedge C_{sh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(D, \sigma(y)))$. In this output transition, the program sends the response in variable y through channel D. C_{sh} holds because from Q_{l_5} we have $isRaRes(y)$ and $isValidCap(y.cap)$. In addition, function f_2 release the tree token. Hence, this verification holds.

Finally, the post-condition of program I_{sh} is satisfied because $Q_t \rightarrow \psi_{sh}$.

When program O receives the response, the program processes and forwards the response as explained in section 6.4.1. Finally, program P_{ra} adds the capability to its capability set as described in section 5.4.

□

6.4.2 Second Lemma: Internal Delegation

Second lemmas indicates that the internal delegation of a valid p-cap by a process creates a valid p-cap for another process inside the same node. Hence, the intermediate controller handles the internal delegation inside the node. We formally define the lemma and proof it.

Lemma 7. *Given two processes with unique IDs inside a process node and a intermediate controller in the same node, if the first process delegates a valid p-cap to second one, then the second process will get a valid p-cap as the result of the delegation request.*

Proof. We use Assumption-Commitment technique to prove the lemma.

The proof of program O is explained in section 6.4.1.

Program I_{qh} receives a request from the operating system via channel A and finds out the request is internal delegation one. Then, I_{qh} forwards the request to program I_{id}, receives the response from it, and forwards the response toward the response handler through channel E.

The A-C formula for program I_{qh} is as follows:

$$\vdash \langle Ass_{qh},\ C_{qh} \rangle\ \{\varphi_{qh}\}\ I_{qh}\ \{\psi_{qh}\}$$

The assertion network for I_{qh} is as follows:

$$Q_s \stackrel{\text{def}}{=} \#A = 0\ \wedge\ \#E = 0\ \wedge\ \#A_{id} = \#B_{id} = \#C_{id} = 0 \wedge \neg hasTreeToken$$

$$Q_{l_1} \stackrel{\text{def}}{=} \#A_{id} = \#B_{id} = \#C_{id}\ \wedge\ \neg hasTreeToken$$

$$Q_{l_2} \stackrel{\text{def}}{=} \#A_{id} = \#B_{id} = \#C_{id}\ \wedge\ last(A) = x$$

$$Q_{l_5} \stackrel{\text{def}}{=} \#A_{id} = \#B_{id} = \#C_{id}\ \wedge\ last(A) = x \wedge isIdRes(last(A))\ \wedge\ hasTreeToken$$

$$Q_{l_6} \stackrel{\text{def}}{=} (\#A_{id} - 1) = \#B_{id} = \#C_{id}\ \wedge\ last(A) = x \wedge last(A_{id}) = x$$

$$Q_{l_7} \stackrel{\text{def}}{=} \#A_{id} = \#B_{id} = (\#C_{id} + 1)\ \wedge\ last(A) = x \wedge last(A_{id}) = x\ \wedge\ last(B_{id}) = y$$

$$Q_{l_8} \stackrel{\text{def}}{=} \#A_{id} = \#B_{id} = (\#C_{id} + 1)\ \wedge\ last(A) = x \wedge last(A_{id}) = x\ \wedge\ last(B_{id}) = y\ \wedge\ last(E) = y$$

$$Q_{l_9} \stackrel{\text{def}}{=} \#A_{id} = \#B_{id} = \#C_{id}\ \wedge\ last(A) = x \wedge last(A_{id}) = x\ \wedge\ last(B_{id}) = y\ \wedge\ last(C_{id}) = z\ \wedge\ last(E) = y$$

$$Q_t \stackrel{\text{def}}{=} false$$

We check the following verifications to prove that above assertion network is an A-C-inductive assertion network w.r.t. assumption Ass_{qh}, commitment C_{qh}, and channels A, E, A_{id}, B_{id}, and C_{ra}.

- $\models Q_s \rightarrow C_{qh}$ follows from the above definition.
- $\models Q_s\ \wedge\ Ass_{qh} \rightarrow Q_{l_1}\ \circ\ init$. In this internal transition, function *init* does not change the state of the program. Hence, this verification holds.
- $\models Q_{l_1}\ \wedge\ Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_2})\ \wedge\ C_{qh}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x,\ h \mapsto v,\ \sigma(h).(A, v))$ for arbitrary value $v \in MSG$. In this input transition, $\sigma' \models \#A > 0$ holds because just a communication through channel A took place. Function g assigns the received value to variable x. Since $\#A > 0$, the first implication of Ass_{qh} satisfies $isUniquePID(last(A).spid)$. Thus, this verification holds.

- $\models Q_{l_2} \wedge isIdRes(x) \wedge Ass_{sh} \rightarrow Q_{l_5} \circ f_1$. In this internal transition, function f_1 gets the tree token. Since $\#A > 0$, the condition of the transition we have $isIdRes(last(A))$. Thus, this verification holds.

- $\models Q_{l_5} \wedge Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_6}) \wedge C_{qh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A_{id}, \sigma(x)))$. In this output transition, the request in variable x is forwarded toward internal-delegation module through channel A_{id} because from the condition we have $isIdRes(x)$. C_{qh} is satisfied because $\#A_{id} > 0$ and from Q_{l_5} we have $isIdRes(last(A_{id}))$. Hence, the sender and the receiver processes have unique IDs and are in the current node. Thus, this verification holds.

- $\models Q_{l_6} \wedge Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_7}) \wedge C_{qh}) \circ g)$where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : y,\ h \mapsto v,\ \sigma(h).(B_{id}, v))$ for arbitrary value $v \in MSG$. In this input transition, the program receives the response of program I_{id} through channel B_{id} and assigns it to variable y via function g. Since $\#B_{id} > 0$, the second implication of Ass_{qh} implies $isIdRes(last(B_{id}))$ and $isValidCap(last(B_{cap}).cap)$. Thus, this verification holds.

  $\models Q_{l_7} \wedge Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_8}) \wedge C_{qh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(E, \sigma(y)))$. In this output transition, the program sends the response in variable y through channel E. In addition, C_{qh} holds because from Q_{l_7} and Ass_{qh} we have $isIdRes(y)$ and $isValidCap(last(y).cap)$. Hence, this verification holds.

- $\models Q_{l_8} \wedge Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_8}) \wedge C_{qh}) \circ g)$where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : z,\ h \mapsto v,\ \sigma(h).(C_{id}, v))$ for arbitrary value $v \in MSG$. In this input transition, the program receives another response from program I_{id} through channel C_{id} and assigns it to variable z via function g. Since $\#C_{id} > 0$, the third implication of Ass_{qh} implies $isIdConfRes(last(C_{id}))$ and $isValidCap(last(C_{cap}).cap)$. Thus, this verification holds.

  $\models Q_{l_9} \wedge Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_1}) \wedge C_{qh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(E, \sigma(z)))$. In this output transition, the program sends the response in variable z through channel E. C_{qh} holds because from Ass_{qh} we have $isIdConfRes(z)$ and $isValidCap(z.cap)$. In addition, function f_2 release the tree token. Hence, this verification holds.

Finally, the post-condition of program I_{qh} is satisfied because $Q_t \rightarrow \psi_{qh}$.

Program I_{sh} receives two responses from program I_{qh} via channel E. In this case, I_{sh} just forwards the responses to program O via channel D.

The A-C formula for program I_{sh} is as follows:

$$\vdash \langle Ass_{sh},\ C_{sh} \rangle\ \{\varphi_{sh}\}\ I_{sh}\ \{\psi_{sh}\}$$

where φ_{qh}, ψ_{qh} , Ass_{qh}, and C_{qh} are formalised as follows:

$$\varphi_{sh} \stackrel{\text{def}}{=} \#E = \#D = 0$$
$$\psi_{sh} \stackrel{\text{def}}{=} false$$
$$Ass_{sh} \stackrel{\text{def}}{=} true$$
$$C_{sh} \stackrel{\text{def}}{=} true$$

The assertion network for I_{sh} is as follows:

$$Q_s \stackrel{\text{def}}{=} \#E = \#D = 0$$
$$Q_{l_1} \stackrel{\text{def}}{=} \#E \geq 0 \ \wedge \ \#D \geq 0$$
$$Q_{l_{15}} \stackrel{\text{def}}{=} \#E > 0 \ \wedge \ \#D \geq 0 \ \wedge \ last(E) = x$$
$$Q_t \stackrel{\text{def}}{=} false$$

We check the following verifications to prove that above assertion network is an A-C-inductive assertion network w.r.t. assumption Ass_{sh}, commitment C_{sh}, and channels E and D.

- $\models Q_s \rightarrow C_{sh}$ follows from the above definition.
- $\models Q_s \ \wedge \ Ass_{sh} \rightarrow Q_{l_1} \circ init$. In this internal transition, function *init* does not change the state of the program. Hence, this verification holds.
- $\models Q_{l_1} \ \wedge \ Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_15}) \ \wedge \ C_{sh}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x, \ h \mapsto v, \ \sigma(h).(E, v))$ for arbitrary value $v \in MSG$. In this input transition, just a communication through channel E took place. Function g assigns the received value to variable x, hence $last(E) = x$. Thus, this verification holds.
- $\models Q_{l_15} \wedge Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_1}) \wedge C_{sh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(D, \sigma(x)))$. In this output transition, the response in variable x is just forwarded toward program O through channel D. Thus, this verification holds.

Finally, the post-condition of program I_{H_s} is satisfied because $Q_t \rightarrow \psi_{h_s}$.

When program O receives both responses, the program processes and forwards the responses as explained in section 6.4.1. Finally, programs P_1 and P_2 add the confirmation and the capability to their capability sets as described in section 5.5.

□

6.4.3 Third Lemma: External Delegation

Third lemmas indicates that the external delegation of a valid p-cap by a process creates a valid p-cap for another process inside another node. Hence, both intermediate controllers of the process nodes and the resource controller of the resource node handle the external delegation together. We formally define the lemma and proof it.

Lemma 8. *Given two processes with unique IDs in different process nodes, delegation of a valid capability from the first process to the second process causes that the delegating and the receiving processes receive a valid indicator and a valid p-cap, respectively.*

Proof. We use Assumption-Commitment technique to prove the lemma.

Program I_{qh} receives a request from the delegator program via channel A and finds out the request is a external-delegation one. Then, I_{qh} forwards the request to program

I^q_{ed}, receives the response from it, and forwards the response toward program R through channel C.

The A-C formula for program I_{qh} is as follows:

$$\vdash \langle Ass_{qh},\ C_{qh}\rangle\ \{\varphi_{qh}\}\ I_{qh}\ \{\psi_{qh}\}$$

where φ_{qh}, ψ_{qh} , Ass_{qh}, and C_{qh} are formalised as follows:

$$\begin{aligned}
\varphi_{qh} &\stackrel{\text{def}}{=} \#A = \#C = 0\ \wedge\ \#A^q_{ed} = \#B^q_{ed}\\
\psi_{qh} &\stackrel{\text{def}}{=} false\\
Ass_{qh} &\stackrel{\text{def}}{=} (\#A > 0\ \wedge\ isEdReq(last(A)) \rightarrow\\
&\quad isUniquePID(last(A).spid)\ \wedge\ isValidCap(last(A).cap)) \wedge\\
&\quad (\#B^q_{ed} > 0 \rightarrow\\
&\quad isEdReq(last(B^q_{ed}))\ \wedge\ isValidCap(last(B^q_{ed}).cap))\\
C_{qh} &\stackrel{\text{def}}{=} (\#B > 0 \rightarrow isEdReq(last(B))\ \wedge\ isValidCap(last(B).cap)) \wedge\\
&\quad (\#A^q_{ed} > 0 \rightarrow\\
&\quad isEdReq(last(A^q_{ed}))\ \wedge\ isValidCap(last(A^q_{ed}).cap))
\end{aligned}$$

The assertion network for I_{qh} is as follows:

$$\begin{aligned}
Q_s &\stackrel{\text{def}}{=} \#A = \#C = 0\ \wedge\ \#A^q_{ed} = \#B^q_{ed} = N_{ed}\\
Q_{l_1} &\stackrel{\text{def}}{=} \#A^q_{ed} = \#B^q_{ed}\\
Q_{l_2} &\stackrel{\text{def}}{=} \#A^q_{ed} = \#B^q_{ed}\ \wedge\ last(A) = x\\
Q_{l_3} &\stackrel{\text{def}}{=} (\#A^q_{ed} - 1) = \#B^q_{ed}\ \wedge\ last(A) = x \wedge\\
&\qquad last(A^q_{ed}) = x\\
Q_{l_4} &\stackrel{\text{def}}{=} \#A^q_{ed} = \#B^q_{ed}\ \wedge\ last(A) = x \wedge\\
&\qquad last(A^q_{ed}) = x\ \wedge\ last(B^q_{ed}) = y\\
Q_t &\stackrel{\text{def}}{=} false
\end{aligned}$$

We check the following verifications to prove that above assertion network is an A-C-inductive assertion network w.r.t. assumption Ass_{qh}, commitment C_{qh}, and channels A, B, A_{ra_1}, and B_{ra_1}.

- $\models Q_s \rightarrow C_{qh}$ follows from the above definition.
- $\models Q_s\ \wedge\ Ass_{qh} \rightarrow Q_{l_1}\ \circ\ init$. In this internal transition, function *init* does not change the state of the program. Hence, this verification holds.
- $\models Q_{l_1}\ \wedge\ Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_2})\ \wedge\ C_{qh}) \circ (f_1 \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x,\ h \mapsto v,\ \sigma(h).(A, v))$ for arbitrary value $v \in MSG$. In this input transition, $\sigma' \models \#A > 0$ holds because just a communication through channel A took place. Function g assigns the received value to variable x. Since $\#A > 0$, the first implication of

Ass_{qh} satisfies $isUniquePID(last(A).spid)$ and $isValidCap(last(A).cap)$. Thus, this verification holds.

- $\models Q_{l_2} \wedge isEdReq(x) \wedge Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_{10}}) \wedge C_{qh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A^q_{ed}, \sigma(x)))$. In this output transition, the request in variable x is forwarded toward external-delegation module through channel A^q_{ed} because $isEdReq(x)$ is evaluated to $true$. C_{qh} is satisfied because $\#A^q_{ed} > 0$, from the condition of the transition we have $isEdReq(last(A^q_{ed}))$, and from Q_{l_2} we have $isUniquePID(last(A^q_{ed}).spid)$. Thus, this verification holds.

- $\models Q_{l_{10}} \wedge Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_{11}}) \wedge C_{qh}) \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : y,\ h \mapsto v,\ \sigma(h).(B^q_{ed}, v))$ for arbitrary value $v \in MSG$. In this input transition, the program receives the response of program I_{ed} through channel B^q_{ed} and assign it to variable y via function g. Since $\#B^q_{ed} > 0$, the first implication of Ass_{qh} implies $isEdReq(last(B^q_{ed}))$ and $isValidCap(last(B^q_{ed}).cap)$. Thus, this verification holds.

  $\models Q_{l_{11}} \wedge Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_1}) \wedge C_{qh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B, \sigma(y)))$. In this output transition, the program sends the request in variable y through channel B. C_{qh} holds because from $Q_{l_{11}}$ we have $isEdReq(y)$ and $isValidCap(y.cap)$. Hence, this verification holds.

Finally, the post-condition of program I_{qh} is satisfied because $Q_t \rightarrow \psi_{qh}$.

Program R_h receives a request from program I via channel A and finds out the request is external-delegation one. Then, R_h forwards the request to program R_{ed}, receives the response from it, and forwards the response toward program I through channel B.

The A-C formula for process R_h is as follows:

$$\vdash \langle Ass_h,\ C_h \rangle\ \{\varphi_h\}\ I_h\ \{\psi_h\}$$

where φ_h, ψ_h , Ass_h, and C_h are formalised as follows:

$$\begin{aligned}
\varphi_h &\stackrel{\text{def}}{=} \#A\#B \geq 0 \wedge \#A_{ed} = \#B_{bd} = \#C_{ed} \\
\psi_h &\stackrel{\text{def}}{=} false \\
Ass_h &\stackrel{\text{def}}{=} (\#A > 0 \wedge isEdReq(last(A)) \rightarrow \\
&\quad isUniquePID(last(A).spid) \wedge isValidCap(last(A).cap)) \wedge \\
&\quad (\#B_{ra} > N_{ra} \rightarrow \\
&\quad isEdRes(last(B_{ed})) \wedge isValidCap(last(B_{ed}).cap) \\
&\quad (\#C_{ed} > 0 \rightarrow \\
&\quad isEdConfReq(last(C_{ed})) \wedge isValidCap(last(C_{ed}).cap)) \\
C_h &\stackrel{\text{def}}{=} (\#B > 0 \rightarrow \\
&\quad isEdReq(last(B)) \wedge isValidCap(last(B).cap)) \wedge \\
&\quad (\#A_{ra} > N_{ra} \rightarrow \\
&\quad isEdReq(last(A_{ra})) \wedge isUniquePID(last(A_{ra}).spid))
\end{aligned}$$

The assertion network for R_h is as follows:

$$
\begin{aligned}
Q_s &\stackrel{\text{def}}{=} \#A = \#B = 0 \ \wedge \ \#A_{ed} = \#B_{ed} = \#C_{ed} \\
Q_{l_1} &\stackrel{\text{def}}{=} \#A_{ra} = \#B_{ra} = \#C_{ed} \\
Q_{l_2} &\stackrel{\text{def}}{=} \#A_{ed} = \#B_{ed} = \#C_{ed} \ \wedge \ last(A) = x \\
Q_{l_5} &\stackrel{\text{def}}{=} (\#A_{ra} - 1) = \#B_{ra} = \#C_{ed} \ \wedge \ last(A) = x \\
&\qquad \wedge \ last(A_{ed}) = x \\
Q_{l_6} &\stackrel{\text{def}}{=} \#A^q_{ed} = \#B^q_{ed} = (\#C_{ed} + 1) \ \wedge \ last(A) = x \\
&\qquad \wedge \ last(A_{ed}) = x \ \wedge \ last(B_{ed}) = y \\
Q_{l_7} &\stackrel{\text{def}}{=} \#A^q_{ed} = \#B^q_{ed} \ \wedge \ last(A) = x \ \wedge \ last(A_{ed}) = x \\
&\qquad \wedge \ last(B_{ed}) = y \ \wedge \ last(B) = y \\
Q_{l_8} &\stackrel{\text{def}}{=} \#A^q_{ed} = \#B^q_{ed} \ \wedge \ last(A) = x \ \wedge \ last(A_{ed}) = x \\
&\qquad \wedge \ last(B_{ed}) = y \ \wedge \ last(C_{ed}) = z \ \wedge \ last(B) = y \\
Q_t &\stackrel{\text{def}}{=} false
\end{aligned}
$$

- $\models Q_s \rightarrow C_h$ follows from the above definition.
- $\models Q_s \ \wedge \ Ass_h \rightarrow Q_{l_1} \ \circ \ init$. In this internal transition, function *init* does not change the state of the program. Hence, this verification holds.
- $\models Q_{l_1} \wedge Ass_h \rightarrow ((Ass_h \rightarrow Q_{l_2}) \wedge C_h) \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x, h \mapsto v, \sigma(h).(M, v))$ for arbitrary value $v \in MSG$. In this input transition, the program receives a message through channel M and function g stores it in variable x. Based on Ass_h, we have $isUniquePID(last(x).spid))$. Thus, this verification holds.
- $\models Q_{l_2} \ \wedge \ isEdReq(x) \ \wedge \ Ass_h \rightarrow ((Ass_h \rightarrow Q_{l_5}) \ \wedge \ C_h))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A_{ed}, \sigma(x)))$. In this output transition, the request in variable x is forwarded toward resource-allocation module through channel $\#A_{ed}$ because $isEdReq(x)$ is evaluated to *true*. C_h is satisfied because $\#A_{ed} > 0$, from the condition of the transition we have $isEdReq(last(A_{ed}))$, and from Q_{l_2} we have $isUniquePID(last(A_{ed}).spid)$. Thus, this verification holds.

  $\models Q_{l_5} \wedge Ass_h \rightarrow ((Ass_h \rightarrow Q_{l_6}) \wedge C_h))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B_{ed}\sigma(y)))$. In this input transition, the program receives the delegation response in variable y through channel B_{ed}. Hence, this verification holds.

  $\models Q_{l_6} \wedge Ass_h \rightarrow ((Ass_h \rightarrow Q_{l_7}) \wedge C_h))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B, \sigma(y)))$. In this output transition, the program sends the response in variable y through channel B. C_h holds because from Q_{l_6} and Ass_h we have $isEdRes(y)$ and $isValidCap(y.cap)$. Hence, this verification holds.

  $\models Q_{l_7} \wedge Ass_h \rightarrow ((Ass_h \rightarrow Q_{l_8}) \wedge C_h))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(C_{ed}, \sigma(z)))$. In this input transition, the program receives the delegation-confirmation response in variable z through channel C_{ed}. Hence, this verification holds.

$\models Q_{l_8} \wedge Ass_h \rightarrow ((Ass_h \rightarrow Q_{l_1}) \wedge C_h))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B, \sigma(z)))$. In this output transition, the program sends the response in variable z through channel B. C_h holds because from Q_{l_8} and Ass_h we have $isEdConfRes(z)$ and $isValidCap(y.cap)$. Hence, this verification holds.

Finally, the post-condition of program R_h is satisfied because $Q_t \rightarrow \psi_h$.

Program I_{sh} on the receiving-process side receives a response from program R via channel C and finds out it is a delegation response. Then, I_{sh} forwards the response to RD_3 module, receives the response from the module, and forwards the response toward program O via channel D.

The A-C formula for program I_{sh} is as follows:

$$\vdash \langle Ass_{sh},\ C_{sh} \rangle\ \{\varphi_{sh}\}\ I_{sh}\ \{\psi_{sh}\}$$

where φ_{qh}, ψ_{qh} , Ass_{qh}, and C_{qh} are formalised as follows:

$$\begin{aligned}
\varphi_{sh} &\stackrel{\text{def}}{=} \#C = \#D = 0 \ \wedge\ \#A_{rd_3} = \#B_{rd_3} \ \wedge\ \neg hasTreeToken \\
\psi_{sh} &\stackrel{\text{def}}{=} false \\
Ass_{sh} &\stackrel{\text{def}}{=} (\#C > 0 \ \wedge\ isEdRes(last(C)) \rightarrow isValidCap(last(C).cap)) \wedge \\
&\quad (\#B_{rd_3} > 0 \rightarrow \\
&\qquad isEdRes(last(B_{rd_3})) \ \wedge\ isValidCap(last(B_{rd_3}).cap)) \\
C_{sh} &\stackrel{\text{def}}{=} (\#D > 0 \ \wedge\ isEdRes(last(D)) \rightarrow isValidCap(last(D).cap)) \wedge \\
&\quad (\#A_{rd_3} > 0 \rightarrow \\
&\qquad isEdRes(last(A_{rd_3})) \ \wedge\ isValidCap(last(A_{rd_3}).cap))
\end{aligned}$$

The assertion network for I_{sh} is as follows:

$$\begin{aligned}
Q_s &\stackrel{\text{def}}{=} \#C \geq 0 \ \wedge\ \#D \geq 0 \ \wedge\ \#A_{rd_3} = \#B_{rd_3} \ \wedge\ \neg hasTreeToken \\
Q_{l_1} &\stackrel{\text{def}}{=} \#C \geq 0 \ \wedge\ \#D \geq 0 \ \wedge\ \#A_{rd_3} = \#B_{rd_3} \ \wedge\ \neg hasTreeToken \\
Q_{l_2} &\stackrel{\text{def}}{=} \#C > 0 \ \wedge\ \#D \geq 0 \ \wedge\ \#A_{rd_3} = \#B_{rd_3} \ \wedge\ last(C) = x \ \wedge\ \neg hasTreeToken \\
Q_{l_6} &\stackrel{\text{def}}{=} \#C > 0 \ \wedge\ \#D \geq 0 \ \wedge\ \#A_{rd_3} = \#B_{rd_3} \ \wedge\ last(C) = x \ \wedge\ hasTreeToken \\
&\quad isEdRes(x) \ \wedge\ isValidCap(x.cap) \\
Q_{l_7} &\stackrel{\text{def}}{=} \#C > 0 \ \wedge\ \#D \geq 0 \ \wedge\ (\#A_{rd_3} - 1) = \#B^s_{ed} \ \wedge\ last(C) = x \wedge \\
&\quad last(A_{rd_3}) = x \ \wedge\ hasTreeToken \\
Q_{l_8} &\stackrel{\text{def}}{=} \#C > 0 \ \wedge\ \#D \geq 0 \ \wedge\ \#A_{rd_3} = \#B_{rd_3} \ \wedge\ last(C) = x \ \wedge\ last(A_{rd_3}) = x \wedge \\
&\quad last(B_{rd_3}) = y \ \wedge\ hasTreeToken \ \wedge\ isEdRes(y) \ \wedge\ isValidCap(y.cap) \\
Q_t &\stackrel{\text{def}}{=} false
\end{aligned}$$

We check the following verifications to prove that above assertion network is an A-C-inductive assertion network w.r.t. assumption Ass_{sh}, commitment C_{sh}, and channels C, D, A_{rd_3}, and B_{rd_3}.

- $\models Q_s \rightarrow C_{sh}$ follows from the above definition.
- $\models Q_s \ \wedge \ Ass_{sh} \rightarrow Q_{l_1} \ \circ \ init$. In this internal transition, function *init* does not change the state of the program. Hence, this verification holds.
- $\models Q_{l_1} \ \wedge \ Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_2}) \ \wedge \ C_{sh}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x, \ h \mapsto v, \ \sigma(h).(C, v))$ for arbitrary value $v \in MSG$. In this input transition, just a communication through channel C took place. Function g assigns the received value to variable x, hence $last(C) = x$. Thus, this verification holds.
- $\models Q_{l_2} \ \wedge \ isEdRes(x) \ \wedge \ Ass_{sh} \rightarrow Q_{l_6} \ \circ \ f_1$. In this internal transition, function f_1 gets the tree token. Since $\#C > 0$ and $isEdRes(x)$, from Ass_{sh} we have $isValidCap(x.cap)$). Thus, this verification holds.
- $\models Q_{l_6} \wedge Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_7}) \wedge C_{sh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A_{rd_3}, \sigma(x)))$. In this output transition, the response in variable x is forwarded toward resource-allocation module through channel A_{rd_3}. C_{qh} is satisfied because $\#A_{rd_3} > 0$ and from Q_{l_6} we have $isEdRes(last(A_{rd_3}))$ and $isValidCap(last(A_{rd_3}).cap)$. Thus, this verification holds.
- $\models Q_{l_7} \ \wedge \ Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_9}) \ \wedge \ C_{sh}) \circ g)$where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : y, \ h \mapsto v, \ \sigma(h).(B_{rd_3}, v))$ for arbitrary value $v \in MSG$. In this input transition, the program receives the response of program RD_3 through channel B_{rd_3} and assign it to variable y via function g. Since $\#B_{rd_3} > 0$, the first implication of Ass_{sh} implies $isEdRes(last(B^s_{ed}))$ and $isValidCap(last(B_{rd_3}).cap)$. Thus, this verification holds.

  $\models Q_{l_9} \wedge Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_1}) \wedge C_{sh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(D, \sigma(y)))$. In this output transition, the program sends the response in variable y through channel D. C_{sh} holds because from Ass_{sh} we have $isRaRes(B_{rd_3})$ and $isValidCap(last(B_{rd_3}).cap)$. In addition, function f_2 release the tree token. Hence, this verification holds.

Finally, the post-condition of program I_{sh} is satisfied because $Q_t \rightarrow \psi_{sh}$.

When program O receives both responses, the program processes and forwards the responses as explained in section 6.4.1. Then, programs P' receives and adds the new capability to its capability set as described in section 5.6.

Program I_{sh} on the delegating-process side receives a response from program R via channel C and finds out it is a delegation-confirmation response. Then, I_{sh} forwards the response to RD_2 module, receives the response from the module, and forwards the response toward program O via channel D.

The A-C formula for program I_{sh} is as follows:

$$\vdash \langle Ass_{sh}, \ C_{sh} \rangle \ \{\varphi_{sh}\} \ I_{sh} \ \{\psi_{sh}\}$$

$$\begin{aligned}
\varphi_{sh} \quad &\stackrel{\text{def}}{=} \quad \#C > 0 \ \wedge \ \#D > 0 \ \wedge \ \#A^s_{ed} = \#B^s_{ed} \ \wedge \ \neg hasTreeToken \\
\psi_{sh} \quad &\stackrel{\text{def}}{=} \quad false \\
Ass_{sh} \quad &\stackrel{\text{def}}{=} \quad (\#C > 0 \ \wedge \ isEdConfRes(last(C)) \rightarrow isValidCap(last(C).cap)) \wedge \\
&\qquad (\#B^s_{ed} > 0 \rightarrow \\
&\qquad\quad isEdConfRes(last(B^s_{ed})) \ \wedge \ isValidCap(last(B^s_{ed}).cap))
\end{aligned}$$

$$C_{sh} \stackrel{\text{def}}{=} (\#D > 0 \ \wedge \ isEdConfRes(last(D)) \rightarrow isValidCap(last(D).cap)) \wedge (\#A^s_{ed} > 0 \rightarrow isEdConfRes(last(A^s_{ed})) \ \wedge \ isValidCap(last(A^s_{ed}).cap))$$

The assertion network for I_{sh} is as follows:

$$Q_s \stackrel{\text{def}}{=} \#C \geq 0 \ \wedge \ \#D \geq 0 \ \wedge \ \#A^s_{ed} = \#B^s_{ed} \ \wedge \ \neg hasTreeToken$$

$$Q_{l_1} \stackrel{\text{def}}{=} \#C \geq 0 \ \wedge \ \#D \geq 0 \ \wedge \ \#A^s_{ed} = \#B^s_{ed} \ \wedge \ \neg hasTreeToken$$

$$Q_{l_2} \stackrel{\text{def}}{=} \#C > 0 \ \wedge \ \#D \geq 0 \ \wedge \ \#A^s_{ed} = \#B^s_{ed} \ \wedge \ last(C) = x \ \wedge \ \neg hasTreeToken$$

$$Q_{l_9} \stackrel{\text{def}}{=} \#C > 0 \ \wedge \ \#D \geq 0 \ \wedge \ \#A^s_{ed} = \#B^s_{ed} \ \wedge \ last(C) = x \ \wedge \ hasTreeToken \ isEdConfRes(x) \ \wedge \ isValidCap(x.cap)$$

$$Q_{l_{10}} \stackrel{\text{def}}{=} \#C > 0 \ \wedge \ \#D \geq 0 \ \wedge \ (\#A^s_{ed} - 1) = \#B^s_{ed} \ \wedge \ last(C) = x \wedge last(A^s_{ed}) = x \ \wedge \ hasTreeToken$$

$$Q_{l_{11}} \stackrel{\text{def}}{=} \#C > 0 \ \wedge \ \#D \geq 0 \ \wedge \ \#A^s_{ed} = \#B^s_{ed} \ \wedge \ last(C) = x \ \wedge \ last(A^s_{ed}) = x \wedge last(B^s_{ed}) = y \ \wedge \ hasTreeToken \ \wedge \ isEdConfRes(y) \wedge isValidCap(y.cap)$$

$$Q_t \stackrel{\text{def}}{=} false$$

We check the following verifications to prove that above assertion network is an A-C-inductive assertion network w.r.t. assumption Ass_{sh}, commitment C_{sh}, and channels C, D, A^s_{ed}, and B^s_{ed}.

- $\models Q_s \rightarrow C_{sh}$ follows from the above definition.
- $\models Q_s \ \wedge \ Ass_{sh} \rightarrow Q_{l_1} \circ init$. In this internal transition, function *init* does not change the state of the program. Hence, this verification holds.
- $\models Q_{l_1} \ \wedge \ Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_2}) \ \wedge \ C_{sh}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x, \ h \mapsto v, \ \sigma(h).(C, v))$ for arbitrary value $v \in MSG$. In this input transition, just a communication through channel C took place. Function g assigns the received value to variable x, hence $last(C) = x$. Thus, this verification holds.
- $\models Q_{l_2} \ \wedge \ isEdConfRes(x) \ \wedge \ Ass_{sh} \rightarrow Q_{l_6} \circ f_1$. In this internal transition, function f_1 gets the tree token. Since $\#C > 0$ and $isEdRes(x)$, from Ass_{sh} we have $isValidCap(x.cap)$). Thus, this verification holds.
- $\models Q_{l_6} \wedge Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_7}) \wedge C_{sh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A^s_{ed}, \sigma(x)))$. In this output transition, the response in variable x is forwarded toward resource-allocation module through channel A^s_{ed}. C_{qh} is satisfied because $\#A^s_{ed} > 0$ and from Q_{l_6} we have $isEdConfRes(last(A^s_{ed}))$ and $isValidCap(last(A^s_{ed}).cap)$. Thus, this verification holds.
- $\models Q_{l_7} \ \wedge \ Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_9}) \ \wedge \ C_{sh}) \circ g)$where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : y, \ h \mapsto v, \ \sigma(h).(B^s_{ed}, v))$ for arbitrary value $v \in MSG$. In this input transition, the program receives the response of program RD_2 through channel B^s_{ed} and assign it to

variable y via function g. Since $\#B^s_{ed} > 0$, the first implication of Ass_{sh} implies $isEdConfRes(last(B^s_{ed}))$ and $isValidCap(last(B^s_{ed}).cap)$. Thus, this verification holds.

$\models Q_{l_9} \wedge Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_1}) \wedge C_{sh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(D, \sigma(y)))$. In this output transition, the program sends the response in variable y through channel D. C_{sh} holds because from Ass_{sh} we have $isEdConfRes(B^s_{ed})$ and $isValidCap(last(B^s_{ed}).cap)$. In addition, function f_2 release the tree token. Hence, this verification holds.

Finally, the post-condition of program I_{sh} is satisfied because $Q_t \rightarrow \psi_{sh}$.

When program O receives the response, the program processes and forwards the response as explained in section 6.4.1. Finally, program P adds the confirmation capability to its capability set as described in section 5.6.

□

6.4.4 Forth Lemma: Internal Revocation

Forth lemmas indicates that the internal revocation of a valid p-cap by the delegator process will invalidate the delegated p-cap to another process inside the same node. Since the p-cap is delegated internally, the intermediate controller handles the revocation alone. We formally define the lemma and proof it.

Lemma 9. *Given a process with unique ID in a process node and a intermediate controller in the same process node, revoking a delegated p-cap to another process inside the same node invalidates the delegated p-cap .*

Proof. We use Assumption-Commitment technique to prove the lemma.

Program I_{qh} receives the request of a process via channel A and finds out the request is internal revocation one. Then, I_{qh} forwards the request to I_{ir} module, receives the response from it, and forwards the response toward the response handler through channel E. The A-C formula for program I_{qh} is as follows:

$$\vdash \langle Ass_{qh},\ C_{qh} \rangle\ \{\varphi_{qh}\}\ I_{qh}\ \{\psi_{qh}\}$$

$$\begin{aligned}
\varphi_{qh} &\stackrel{\text{def}}{=} \#A = \#E = 0\ \wedge\ \#A_{ir} = \#B_{ir} = N_{ir}\ \wedge \\
&\quad \neg hasTreeToken \\
\psi_{qh} &\stackrel{\text{def}}{=} false \\
Ass_{qh} &\stackrel{\text{def}}{=} (\#A > 0\ \wedge\ isIrReq(Last(A)) \rightarrow \\
&\quad isUniquePID(last(A).spid))\ \wedge\ isValidCap(last(A).cap))\ \wedge \\
&\quad (\#B_{ir} > 0 \rightarrow isIrConfRes(last(B_{ir})) \\
C_{qh} &\stackrel{\text{def}}{=} (\#E > 0 \rightarrow isIrConfRes(last(E))\ \wedge \\
&\quad (\#A_{ir} > 0 \rightarrow isIrReq(last(A_{ir}))\ \wedge\ isValidCap(last(A_{ir}).cap)
\end{aligned}$$

wherein N_{ir} is a logical variable.
The assertion network for I_{qh} is as follows:

$$Q_s \stackrel{\text{def}}{=} \#A = \#E \geq 0 \ \wedge \ \#A_{ir} = \#B_{ir} = 0 \wedge \neg hasTreeToken$$

$$Q_{l_1} \stackrel{\text{def}}{=} \#A_{ir} = \#B_{ir} \ \wedge \ \neg hasTreeToken$$

$$Q_{l_2} \stackrel{\text{def}}{=} \#A_{ir} = \#B_{ir} \ \wedge \ last(A) = x$$

$$Q_{l_{12}} \stackrel{\text{def}}{=} \#A_{ir} = \#B_{ir} = \#C_{ir} \ \wedge \ last(A) = x \wedge isIrReq(last(A)) \ \wedge \ hasTreeToken$$

$$Q_{l_{13}} \stackrel{\text{def}}{=} (\#A_{ir} - 1) = \#B_{ir} \ \wedge \ last(A) = x \ \wedge \ last(A_{ir}) = x$$

$$Q_{l_{14}} \stackrel{\text{def}}{=} \#A_{ir} = \#B_{ir} \ \wedge \ last(A) = x \ \wedge \ last(A_{ir}) = x \wedge last(B_{ir}) = y$$

$$Q_t \stackrel{\text{def}}{=} false$$

- $\models Q_s \rightarrow C_{qh}$ follows from the above definition.
- $\models Q_s \ \wedge \ Ass_{qh} \rightarrow Q_{l_1} \ \circ \ init$. In this internal transition, function *init* does not change the state of the program. Hence, this verification holds.
- $\models Q_{l_1} \ \wedge \ Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_2}) \ \wedge \ C_{qh}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x, \ h \mapsto v, \ \sigma(h).(A, v))$ for arbitrary value $v \in MSG$. In this input transition, $\sigma' \models \#A > 0$ holds because just a communication through channel A took place. Function g assigns the received value to variable x. Thus, this verification holds.
- $\models Q_{l_2} \ \wedge \ isLDReq(x) \ \wedge \ Ass_{sh} \rightarrow Q_{l_{12}} \ \circ \ f_1$. In this internal transition, function f_1 gets the tree token. In addition, we have $isUniquePID(last(A).spid))$ and $isValidCap(last(A).cap))$ because $\#A > 0$ and the condition states that $isIrReq(last(A))$. Thus, this verification holds.
- $\models Q_{l_{12}} \ \wedge \ Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_{13}}) \ \wedge \ C_{qh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A_{ir}, \sigma(x)))$. In this output transition, the request in variable x is forwarded toward internal-revocation module through channel A_{ir} because from the condition we have $isIrReq(x)$. C_{qh} is satisfied because $\#A_{ir} > 0$, $last(A) = last(A_{ir}) = x$, and from Ass_{qh} we have $isUniquePID(last(A).spid))$ and $isValidCap(last(A).cap))$. Thus, this verification holds.
- $\models Q_{l_{13}} \ \wedge \ Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_{14}}) \ \wedge \ C_{qh}) \circ g)$where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : y, \ h \mapsto v, \ \sigma(h).(B_{ir}, v))$ for arbitrary value $v \in MSG$. In this input transition, the program receives the response of program I_{ir} through channel B_{ir} and assigns it to variable y via function g. Since $\#B_{ir} > 0$, the second implication of Ass_{qh} implies $isIrConfRes(last(B_{ir}))$. Thus, this verification holds.

  $\models Q_{l_{14}} \wedge Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_1}) \wedge C_{qh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(E, \sigma(y)))$. In this output transition, the program sends the response in variable y through channel E. C_{qh} holds because from Ass_{qh} we have $isIrConfRes(y)$. In addition, function f_2 release the tree token. Hence, this verification holds.

Finally, the post-condition of program I_{qh} is satisfied because $Q_t \rightarrow \psi_{qh}$.

Program I_{sh} receives the response from program I_{qh} via channel E. In this case, I_{sh} just forwards the response to program O via channel B.

The A-C formula for program I_{sh} is as follows:

$$\vdash \langle Ass_{sh},\ C_{sh}\rangle\ \{\varphi_{sh}\}\ I_{sh}\ \{\psi_{sh}\}$$

where φ_{sh}, ψ_{sh} , Ass_{sh}, and C_{sh} are formalised as follows:

$$\varphi_{sh} \stackrel{\text{def}}{=} \#E = \#B = 0$$
$$\psi_{sh} \stackrel{\text{def}}{=} false$$
$$Ass_{sh} \stackrel{\text{def}}{=} true$$
$$C_{sh} \stackrel{\text{def}}{=} true$$

The assertion network for I_{sh} is as follows:

$$Q_s \stackrel{\text{def}}{=} \#E = \#B = 0$$
$$Q_{l_1} \stackrel{\text{def}}{=} \#E \geq 0\ \wedge\ \#B \geq 0$$
$$Q_{l_{15}} \stackrel{\text{def}}{=} \#E > 0\ \wedge\ \#B \geq 0\ \wedge\ last(E) = x$$
$$Q_t \stackrel{\text{def}}{=} false$$

We check the following verifications to prove that above assertion network is an A-C-inductive assertion network w.r.t. assumption Ass_{sh}, commitment C_{sh}, and channels E and B.

- $\models Q_s \rightarrow C_{sh}$ follows from the above definition.
- $\models Q_s\ \wedge\ Ass_{sh} \rightarrow Q_{l_1}\ \circ\ init$. In this internal transition, function *init* does not change the state of the program. Hence, this verification holds.
- $\models Q_{l_1}\ \wedge\ Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_15})\ \wedge\ C_{sh}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x,\ h \mapsto v,\ \sigma(h).(E, v))$ for arbitrary value $v \in MSG$. In this input transition, just a communication through channel E took place. Function g assigns the received value to variable x, hence $last(E) = x$. Thus, this verification holds.
- $\models Q_{l_15} \wedge Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_1}) \wedge C_{sh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(D, \sigma(x)))$. In this output transition, the response in variable x is just forwarded toward program O through channel D. Thus, this verification holds.

Finally, the post-condition of program I_{sh} is satisfied because $Q_t \rightarrow \psi_{sh}$.

When program O receives both responses, the program processes and forwards the responses as explained in section 6.4.1. Finally, programs P receives the confirmation and delete the capability from its capability set as described in section **??**.

□

6.4.5 Fifth Lemma: External Revocation

Fifth lemmas indicates that the external revocation of a valid p-cap by a delegator process will invalidate the delegated p-cap to the receiving process inside another node. In this operation, the intermediate controller on the delegator-process side and the resource controller of the resource node handle the external revocation together. We formally define the lemma and proof it.

Lemma 10. *Given a process with a unique ID in a process node, revocation of a valid delegated capability by the process will revoke the delegated p-cap.*

Proof. We use Assumption-Commitment technique to prove the lemma.

Program I_{qh} receives the request from a process via channel A and finds out the request is external revocation one. Then, I_{qh} forwards the request to program R, receives the response from it, and forwards the response toward program R through channel C. The A-C formula for program I_{qh} is as follows:

$$\vdash \langle Ass_{qh},\ C_{qh} \rangle\ \{\varphi_{qh}\}\ I_{qh}\ \{\psi_{qh}\}$$

$$\begin{aligned}
\varphi_{qh} &\stackrel{\text{def}}{=} \#A = \#C = 0\ \wedge\ \#A^q_{er} = \#B^q_{er} \\
\psi_{qh} &\stackrel{\text{def}}{=} false \\
Ass_{qh} &\stackrel{\text{def}}{=} (\#A > 0\ \wedge\ isErReq(Last(A))) \rightarrow \\
&\quad isUniquePID(last(A).spid))\ \wedge\ isValidCap(last(A).cap)) \wedge \\
&\quad (\#B_{rr} > 0 \rightarrow isErReq(last(B_{ld}))) \\
C_{qh} &\stackrel{\text{def}}{=} (\#B > 0 \rightarrow isErReq(last(O))) \wedge \\
&\quad (\#A^q_{er} > 0 \rightarrow isErReq(last(A^q_{er}))\ \wedge\ isUniquePID(last(A).spid)) \wedge \\
&\quad isValidCap(last(A_{ld}).cap))
\end{aligned}$$

The assertion network for I_{qh} is as follows:

$$\begin{aligned}
Q_s &\stackrel{\text{def}}{=} \#A = \#B = 0\ \wedge\ \#A^q_{er} = \#B^q_{er} = 0 \\
Q_{l_1} &\stackrel{\text{def}}{=} \#A^q_{er} = \#B^q_{er} \\
Q_{l_2} &\stackrel{\text{def}}{=} \#A^q_{er} = \#B^q_{er}\ \wedge\ last(A) = x \\
Q_{l_{15}} &\stackrel{\text{def}}{=} (\#A^q_{er} - 1) = \#B^q_{er}\ \wedge\ last(A) = x \wedge \\
&\qquad last(A^q_{er}) = x \\
Q_{l_{16}} &\stackrel{\text{def}}{=} \#A^q_{er} = \#B^q_{er}\ \wedge\ last(A) = x \wedge \\
&\qquad last(A^q_{er}) = x\ \wedge\ last(B^q_{er}) = y \\
Q_t &\stackrel{\text{def}}{=} false
\end{aligned}$$

We check the following verifications to prove that above assertion network is an A-C-inductive assertion network w.r.t. assumption Ass_{qh}, commitment C_{qh}, and channels A, C, A^q_{er}, and B^q_{er}.

- $\models Q_s \rightarrow C_{qh}$ follows from the above definition.
- $\models Q_s \wedge Ass_{qh} \rightarrow Q_{l_1} \circ init$. In this internal transition, function *init* does not change the state of the program. Hence, this verification holds.
- $\models Q_{l_1} \wedge Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_2}) \wedge C_{qh}) \circ (f_1 \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x,\ h \mapsto v,\ \sigma(h).(A, v))$ for arbitrary value $v \in MSG$. In this input transition, $\sigma' \models \#A > 0$ holds because just a communication through channel A took place. Function g assigns the received value to variable x. Thus, this verification holds.
- $\models Q_{l_2} \wedge isErReq(x) \wedge Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_{15}}) \wedge C_{qh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A_{rr}, \sigma(x)))$. In this output transition, the request in variable x is forwarded toward resource-allocation module through channel A_{rr} because $isErReq(x)$ is evaluated to *true*. C_{qh} is satisfied because $\#A_{rr} > 0$, from the condition of the transition we have $isErReq(last(A_{rr}))$, and from Ass_{qh} we have $isUniquePID(last(A_{rr}).spid)$ and $isValidCap(last(A_{rr}).cap)$. Thus, this verification holds.
- $\models Q_{l_{15}} \wedge Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_{16}}) \wedge C_{qh}) \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : y,\ h \mapsto v,\ \sigma(h).(B_{rr}, v))$ for arbitrary value $v \in MSG$. In this input transition, the program receives the response of program I_{rr} through channel B_{rr} and assign it to variable y via function g. Since $\#B_{rr} > 0$, the first implication of Ass_{qh} implies $isErReq(last(B_{rr}))$ and $isValidCap(last(B_{rr}).cap)$. Thus, this verification holds.

  $\models Q_{l_{16}} \wedge Ass_{qh} \rightarrow ((Ass_{qh} \rightarrow Q_{l_1}) \wedge C_{qh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B, \sigma(y)))$. In this output transition, the program sends the request in variable y through channel B. C_{qh} holds because we have $isErReq(y)$ and $isValidCap(y.cap)$. Hence, this verification holds.

Finally, the post-condition of program I_{H_q} is satisfied because $Q_t \rightarrow \psi_{h_q}$.

Program R_h receives a request from program I via channel A and finds out the request is external-revocation one. Then, R_h forwards the request to program R_{er}, receives the response from it, and forwards the response toward program I through channel B.

The A-C formula for process R_h is as follows:

$$\vdash \langle Ass_h,\ C_h \rangle\ \{\varphi_h\}\ I_h\ \{\psi_h\}$$

where φ_h, ψ_h , Ass_h, and C_h are formalised as follows:

$$\begin{aligned}
\varphi_h &\stackrel{\text{def}}{=} \#A = \#B = 0 \ \wedge\ \#A_{er} = \#B_{er} \\
\psi_h &\stackrel{\text{def}}{=} false \\
Ass_h &\stackrel{\text{def}}{=} (\#A > 0 \ \wedge\ isErReq(last(B_{rr})) \rightarrow isValidCap(last(A).cap))) \wedge \\
&\quad (\#B_{er} > 0 \rightarrow \\
&\qquad isErRes(last(B_{er})) \ \wedge\ isErConfRes(last(B_{er}).cap)
\end{aligned}$$

$$C_h \quad \stackrel{\text{def}}{=} \quad (\#B > 0 \rightarrow isErConfRes(last(B))) \wedge (\#A_{er} > 0 \rightarrow isErRes(last(A_{er})) \wedge isValidCap(last(A_{er}.cap).spid))$$

The assertion network for R_h is as follows:

$$Q_s \stackrel{\text{def}}{=} \#A = \#B = 0 \wedge \#A_{er} = \#B_{er}$$

$$Q_{l_1} \stackrel{\text{def}}{=} \#A = \#B \wedge \#A_{er} = \#B_{er}$$

$$Q_{l_2} \stackrel{\text{def}}{=} \#A_{er} = \#B_{er} \wedge last(A) = x$$

$$Q_{l_3} \stackrel{\text{def}}{=} (\#A_{er} - 1) = \#B_{er} \wedge last(A) = x \wedge last(A_{er}) = x$$

$$Q_{l_4} \stackrel{\text{def}}{=} \#A_{er} = \#B_{er} \wedge last(A) = x \wedge last(A_{er}) = x \wedge last(B_{er}) = y$$

$$Q_t \stackrel{\text{def}}{=} false$$

We check the following verifications to prove that above assertion network is an A-C-inductive assertion network w.r.t. assumption Ass_h, commitment C_h, and channels A, B, A_{er}, and B_{er}.

- $\models Q_s \rightarrow C_h$ follows from the above definition.
- $\models Q_s \wedge Ass_h \rightarrow Q_{l_1} \circ init$. In this internal transition, function *init* does not change the state of the program. Hence, this verification holds.
- $\models Q_{l_1} \wedge Ass_h \rightarrow ((Ass_h \rightarrow Q_{l_2}) \wedge C_h) \circ g)$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x, h \mapsto v, \sigma(h).(M, v))$ for arbitrary value $v \in MSG$. In this input transition, the program receives a message through channel A and function g stores it in variable x. Based on Ass_h, we have $isUniquePID(last(x).spid))$. Thus, this verification holds.
- $\models Q_{l_2} \wedge isRAReq(x) \wedge Ass_h \rightarrow ((Ass_h \rightarrow Q_{l_3}) \wedge C_h))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A_{er}, \sigma(x)))$. In this output transition, the request in variable x is forwarded toward resource-allocation module through channel $\#A_{er}$ because $isRAReq(x)$ is evaluated to *true*. C_h is satisfied because $\#A_{er} > 0$, from the condition of the transition we have $isRaReq(last(A_{er}))$, and from Q_{l_2} we have $isUniquePID(last(A_{er}).spid)$. Thus, this verification holds.

  $\models Q_{l_3} \wedge Ass_h \rightarrow ((Ass_h \rightarrow Q_{l_4}) \wedge C_h))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B_{er}\sigma(y)))$. In this input transition, the program receives the resource-allocation response in variable y through channel B_{er}. Hence, this verification holds.

  $\models Q_{l_4} \wedge Ass_h \rightarrow ((Ass_h \rightarrow Q_{l_1}) \wedge C_h))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(B, \sigma(y)))$. In this output transition, the program sends the response in variable y through channel B. C_h holds because from Ass_h we have $isErConfRes(y)$. Hence, this verification holds.

Finally, the post-condition of program R_h is satisfied because $Q_t \rightarrow \psi_h$.

Program I_{sh} on the process side receives a response from program R via channel D and finds out it is a revocation-confirmation response. Then, I_{sh} forwards the response to program I^s_{er} module, receives the response from the module, and forwards the response toward program O via channel B.

The A-C formula for program I_{sh} is as follows:

$$\vdash \langle Ass_{sh},\ C_{sh}\rangle\ \{\varphi_{sh}\}\ I_{sh}\ \{\psi_{sh}\}$$

$$\begin{aligned}
\varphi_{sh} &\stackrel{\text{def}}{=} \#D = \#B = 0\ \wedge\ \#A^s_{er} = \#B^s_{er}\ \wedge\ \neg hasTreeToken\\
\psi_{sh} &\stackrel{\text{def}}{=} false\\
Ass_{sh} &\stackrel{\text{def}}{=} (\#D > 0\ \wedge\ isErConfRes(last(C)) \rightarrow isValidCap(last(C).cap)) \wedge\\
&\quad\ (\#B^s_{er} > 0 \rightarrow isErConfRes(last(B^s_{er})))\\
C_{sh} &\stackrel{\text{def}}{=} (\#B > 0 \rightarrow isErConfRes(last(D))) \wedge\\
&\quad\ (\#A^s_{er} > 0 \rightarrow isErConfRes(last(A^s_{er})))
\end{aligned}$$

The assertion network for I_{sh} is as follows:

$$\begin{aligned}
Q_s &\stackrel{\text{def}}{=} \#D = \#B = 0\ \wedge\ \#A^s_{er} = \#B^s_{er}\ \wedge\ \neg hasTreeToken\\
Q_{l_1} &\stackrel{\text{def}}{=} \#A^s_{er} = \#B^s_{er}\ \wedge\ \neg hasTreeToken\\
Q_{l_2} &\stackrel{\text{def}}{=} \#A^s_{er} = \#B^s_{er}\ \wedge\ last(C) = x\ \wedge\ \neg hasTreeToken\\
Q_{l_{12}} &\stackrel{\text{def}}{=} \#A^s_{er} = \#B^s_{er}\ \wedge\ last(C) = x\ \wedge\ hasTreeToken\\
&\quad\ isErConfRes(x)\\
Q_{l_{13}} &\stackrel{\text{def}}{=} (\#A^s_{er} - 1) = \#B^s_{er}\ \wedge\ last(C) = x \wedge\\
&\quad\ last(A^s_{er}) = x\ \wedge\ hasTreeToken\\
Q_{l_{14}} &\stackrel{\text{def}}{=} \#A^s_{er} = \#B_{rd_2}\ \wedge\ last(C) = x\ \wedge\ last(A^s_{er}) = x \wedge\\
&\quad\ last(B^s_{er}) = y\ \wedge\ hasTreeToken\ \wedge\ isErConfRes(y)\\
Q_t &\stackrel{\text{def}}{=} false
\end{aligned}$$

We check the following verifications to prove that above assertion network is an A-C-inductive assertion network w.r.t. assumption Ass_{sh}, commitment C_{sh}, and channels B, D, A^s_{er}, and B^s_{er}.

- $\models Q_s \rightarrow C_{sh}$ follows from the above definition.
- $\models Q_s\ \wedge\ Ass_{sh} \rightarrow Q_{l_1}\ \circ\ init$. In this internal transition, function *init* does not change the state of the program. Hence, this verification holds.
- $\models Q_{l_1}\ \wedge\ Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_2})\ \wedge\ C_{sh}) \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : x,\ h \mapsto v,\ \sigma(h).(C, v))$ for arbitrary value $v \in MSG$. In this input transition, just a communication through channel C took place. Function g assigns the received value to variable x, hence $last(C) = x$. Thus, this verification holds.

- $\models Q_{l_2} \wedge isRDConfRes(x) \wedge Ass_{sh} \rightarrow Q_{l_{12}} \circ f_1$. In this internal transition, function f_1 gets the tree token. Since $\#C > 0$ from Ass_{sh} we have $isErConfRes(x)$. Thus, this verification holds.
- $\models Q_{l_{12}} \wedge Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_{13}}) \wedge C_{sh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(A^s_{er}, \sigma(x)))$. In this output transition, the response in variable x is forwarded toward external-revocation module through channel A^s_{er}. C_{qh} is satisfied because $\#A^s_{er} > 0$ and from Ass_{sh} we have $isErConfRes(last(A^s_{er}))$. Thus, this verification holds.
- $\models Q_{l_{13}} \wedge Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_{14}}) \wedge C_{sh}) \circ g)$where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : y,\ h \mapsto v,\ \sigma(h).(B^s_{er}, v))$ for arbitrary value $v \in MSG$. In this input transition, the program receives the response of program RR_2 through channel B^s_{er} and assign it to variable y via function g. Since $\#B^s_{er} > 0$, the first implication of Ass_{sh} implies $isErConfRes(last(B^s_{er}))$. Thus, this verification holds.

  $\models Q_{l_{14}} \wedge Ass_{sh} \rightarrow ((Ass_{sh} \rightarrow Q_{l_1}) \wedge C_{sh}))$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h \mapsto \sigma(h).(D, \sigma(y)))$. In this output transition, the program sends the response in variable y through channel D. C_{sh} holds because from Ass_{sh} we have $isErConfRes(B^s_{er})$. In addition, function f_2 release the tree token. Hence, this verification holds.

Finally, the post-condition of program I_{sh} is satisfied because $Q_t \rightarrow \psi_{sh}$.

When program O receives the response, the program processes and forwards the response as explained in section 6.4.1. Finally, program P adds the confirmation capability to its capability set as described in section 5.8.

□

Table 3: Correctness Checks of the Models

Model	Transitions	Depth	Time(sec)	Lines of Code
RA	2224	127	0.01	350
ID	950	106	0.01	349
ED	496828	277	2.15	700
IR	1165	86	0.01	287
ER	26403	140	0.06	380

7 Model Checking

We use the SPIN model checker [29] to check our design. SPIN employs the *PROMELA* language to define models. We built the models of Lemmas 1 to 5 using PROMELA, where each model consists of the following PROMELA object types.

Processes: a process is a *proctype* object type that defines the behavior of programs in the lemmas, such as Ira and Rra (Figure 6).

Channels: a channel models a synchronous messaging channel in the A-C method, using *chan* object type. a channel is a one-way semantic interface between two programs in the lemmas (Figure 6).

Data Objects: PROMELA only supports basic object types, such as *byte* and *short*, but not complex ones, such as *floating-point*.

Claims: a system verification proves what is possible in a model and what is not. PROMELA defines a model's logical correctness using five claim types: *basic assertions*, *meta labels*, *never claims*, and *trace assertions*. We employ basic assertions and trace assertions to check the correctness of our models according to the assumption-commitment method. A Basic assertion includes an expression that PSIN evaluates as False or True during a verification; a False assertion causes the verification to fail. A trace assertion checks if the model has exchanged messages in a specific order and if the exchanged messages include defined data.

We modeled and verified Lemmas 1 to 5, for the general access control system and the MDC instantiated system; SPIN verified all the models as correct. Table 3 depicts the details of each verification

References

[1] Mike Accetta, Robert Baron, William Bolosky, David Golub, Richard Rashid, Avadis Tevanian, and Michael Young. 1986. Mach: A new kernel foundation for UNIX development. (1986).

[2] Mohammad Alizadeh, Shuang Yang, Milad Sharif, Sachin Katti, Nick McKeown, Balaji Prabhakar, and Scott Shenker. 2013. pfabric: Minimal near-optimal datacenter transport. *ACM SIGCOMM Computer Communication Review* 43, 4 (2013), 435–446.

[3] Emmanuel Amaro, Christopher Branner-Augmon, Zhihong Luo, Amy Ousterhout, Marcos K Aguilera, Aurojit Panda, Sylvia Ratnasamy, and Scott Shenker. 2020. Can far memory improve job throughput?. In *Proceedings of the Fifteenth European Conference on Computer Systems*. 1–16.

[4] Sebastian Angel, Mihir Nanavati, and Siddhartha Sen. 2020. Disaggregation and the Application. In *12th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 20)*.

[5] Krste Asanović. 2014. FireBox: A Hardware Building Block for 2020 Warehouse-Scale Computers. *In FAST* (2014).

[6] Leonid Azriel, Lukas Humbel, Reto Achermann, Alex Richardson, Moritz Hoffmann, Avi Mendelson, Timothy Roscoe, Robert NM Watson, Paolo Faraboschi, and Dejan Milojicic. 2019. Memory-side protection with a capability enforcement co-processor. *ACM Transactions on Architecture and Code Optimization (TACO)* 16, 1 (2019), 1–26.

[7] Andrew Baumann, Paul Barham, Pierre-Evariste Dagand, Tim Harris, Rebecca Isaacs, Simon Peter, Timothy Roscoe, Adrian Schüpbach, and Akhilesh Singhania. 2009. The multikernel: a new OS architecture for scalable multicore systems. In *Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles*. 29–44.

[8] Daniel S Berger, Daniel Ernst, Huaicheng Li, Pantea Zardoshti, Monish Shah, Samir Rajadnya, Scott Lee, Lisa Hsu, Ishwar Agarwal, Mark D Hill, et al. 2023. Design Tradeoffs in CXL-Based Memory Pools for Public Cloud Platforms. *IEEE Micro* 43, 2 (2023), 30–38.

[9] Mark S Birrittella, Mark Debbage, Ram Huggahalli, James Kunz, Tom Lovett, Todd Rimmer, Keith D Underwood, and Robert C Zak. 2015. Intel® omni-path architecture: Enabling scalable, high performance fabrics. In *2015 IEEE 23rd Annual Symposium on High-Performance Interconnects*. IEEE, 1–9.

[10] Kirk M Bresniker, Paolo Faraboschi, Avi Mendelson, Dejan Milojicic, Timothy Roscoe, and Robert NM Watson. 2019. Rack-scale capabilities: fine-grained protection for large-scale memories. *Computer* 52, 2 (2019), 52–62.

[11] Blake Caldwell, Sepideh Goodarzy, Sangtae Ha, Richard Han, Eric Keller, Eric Rozner, and Youngbin Im. 2020. Fluidmem: Full, flexible, and fast memory disaggregation for the cloud. In *IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*. 665–677.

[12] Nicholas P Carter, Stephen W Keckler, and William J Dally. 1994. Hardware support for fast capability-based addressing. *ACM SIGOPS Operating Systems Review* 28, 5 (1994), 319–327.

[13] David Cock, Abishek Ramdas, Daniel Schwyn, Michael Giardino, Adam Turowski, Zhenhao He, Nora Hossle, Dario Korolija, Melissa Licciardello, Kristina

Martsenko, et al. 2022. Enzian: an open, general, CPU/FPGA platform for systems software research. In *Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*. 434–451.

[14] George W Cox, William M Corwin, Konrad K Lai, and Fred J Pollack. 1981. A unified model and implementation for interprocess communication in a multiprocessor environment. In *Proceedings of the eighth ACM symposium on Operating systems principles*. 125–126.

[15] Compute Express Link (CXL). 2023 (accessed April 16, 2023). CXL Specification. `https://www.computeexpresslink.org/download-the-specification`.

[16] Karl Czajkowski, Steven Fitzgerald, Ian Foster, and Carl Kesselman. 2001. Grid information services for distributed resource sharing. In *Proceedings 10th IEEE International Symposium on High Performance Distributed Computing*. IEEE, 181–194.

[17] W-P De Roever, Frank de Boer, Ulrich Hanneman, Jozef Hooman, Yassine Lakhnech, Mannes Poel, and Job Zwiers. 2001. *Concurrency verification: Introduction to compositional and non-compositional methods*. Vol. 54. Cambridge University Press.

[18] Jack B Dennis and Earl C Van Horn. 1966. Programming semantics for multiprogrammed computations. *Commun. ACM* 9, 3 (1966), 143–155.

[19] Joe Devietti, Colin Blundell, Milo MK Martin, and Steve Zdancewic. 2008. Hardbound: architectural support for spatial safety of the C programming language. *ACM SIGOPS Operating Systems Review* 42, 2 (2008), 103–114.

[20] Aleksandar Dragojević, Dushyanth Narayanan, Miguel Castro, and Orion Hodson. 2014. FaRM: Fast remote memory. In *11th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 14)*. 401–414.

[21] Robert S. Fabry. 1974. Capability-based addressing. *Commun. ACM* 17, 7 (1974), 403–412.

[22] Peter X Gao, Akshay Narayan, Sagar Karandikar, Joao Carreira, Sangjin Han, Rachit Agarwal, Sylvia Ratnasamy, and Scott Shenker. 2016. Network requirements for resource disaggregation. In *12th USENIX symposium on operating systems design and implementation (OSDI 16)*. 249–264.

[23] Donghyun Gouk, Sangwon Lee, Miryeong Kwon, and Myoungsoo Jung. 2022. Direct access, High-Performance memory disaggregation with DirectCXL. In *2022 USENIX Annual Technical Conference (USENIX ATC 22)*. 287–294.

[24] Juncheng Gu, Youngmoon Lee, Yiwen Zhang, Mosharaf Chowdhury, and Kang G Shin. 2017. Efficient memory disaggregation with infiniswap. In *14th USENIX Symposium on Networked Systems Design and Implementation (NSDI 17)*. 649–667.

[25] Zhiyuan Guo, Yizhou Shan, Xuhao Luo, Yutong Huang, and Yiying Zhang. 2022. Clio: A hardware-software co-designed disaggregated memory system. In *Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*. 417–433.

[26] Norman Hardy. 1985. KeyKOS architecture. *ACM SIGOPS Operating Systems Review* 19, 4 (1985), 8–25.

[27] Nikolas Roman Herbst, Samuel Kounev, and Ralf H Reussner. 2013. Elasticity in Cloud Computing: What It Is, and What It Is Not.. In *ICAC*, Vol. 13. 23–27.

[28] Matthias Hille, Nils Asmussen, Pramod Bhatotia, and Hermann Härtig. 2019. Semperos: A distributed capability system. In *2019 {USENIX} Annual Technical Conference ({USENIX}{ATC} 19)*. 709–722.

[29] Gerard J. Holzmann. 1997. The model checker SPIN. *IEEE Transactions on software engineering* 23, 5 (1997), 279–295.

[30] Merle E Houdek, Frank G Soltis, and Roy L Hoffman. 1981. IBM System/38 support for capability-based addressing. In *Proceedings of the 8th annual symposium on Computer Architecture*. 341–348.

[31] Changho Hwang, Taehyun Kim, Sunghyun Kim, Jinwoo Shin, and Kyoung-Soo Park. 2021. Elastic resource sharing for distributed deep learning. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*. 721–739.

[32] Anita K Jones, Robert J Chansler Jr, Ivor Durham, Karsten Schwans, and Steven R Vegdahl. 1979. StarOS, a multiprocessor operating system for the support of task forces. In *Proceedings of the seventh ACM symposium on Operating systems principles*. 117–127.

[33] Kostas Katrinis, Dimitris Syrivelis, Dionisios Pnevmatikatos, Georgios Zervas, Dimitris Theodoropoulos, Iordanis Koutsopoulos, Kobi Hasharoni, Daniel Raho, Christian Pinto, F Espina, et al. 2016. Rack-scale disaggregated cloud data centers: The dReDBox project vision. In *2016 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 690–695.

[34] Kimberly Keeton. 2015. The machine: An architecture for memory-centric computing. In *Workshop on Runtime and Operating Systems for Supercomputers (ROSS)*, Vol. 10.

[35] Kimberly Keeton. 2017. Memory-Driven Computing.. In *FAST*.

[36] Vamsee Reddy Kommareddy, Clayton Hughes, Simon David Hammond, and Amro Awad. 2021. Deact: Architecture-aware virtual memory support for fabric attached memory systems. In *2021 IEEE International Symposium on High-Performance Computer Architecture (HPCA)*. IEEE, 453–466.

[37] Seung-seob Lee, Yanpeng Yu, Yupeng Tang, Anurag Khandelwal, Lin Zhong, and Abhishek Bhattacharjee. 2021. Mind: In-network memory management for disaggregated data centers. In *Proceedings of the ACM SIGOPS 28th Symposium on Operating Systems Principles*. 488–504.

[38] Sergey Legtchenko, Hugh Williams, Kaveh Razavi, Austin Donnelly, Richard Black, Andrew Douglas, Nathanaël Cheriere, Daniel Fryer, Kai Mast, Angela Demke Brown, et al. 2017. Understanding {Rack-Scale} Disaggregated Storage. In *9th USENIX Workshop on Hot Topics in Storage and File Systems (HotStorage 17)*.

[39] Huaicheng Li, Daniel S Berger, Lisa Hsu, Daniel Ernst, Pantea Zardoshti, Stanko Novakovic, Monish Shah, Samir Rajadnya, Scott Lee, Ishwar Agarwal, et al. 2023. Pond: CXL-based memory pooling systems for cloud platforms. In *Proceedings of the 28th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Volume 2*. 574–587.

[40] Jochen Liedtke. 1995. On micro-kernel construction. *ACM SIGOPS Operating Systems Review* 29, 5 (1995), 237–250.

[41] Kevin Lim, Jichuan Chang, Trevor Mudge, Parthasarathy Ranganathan, Steven K Reinhardt, and Thomas F Wenisch. 2009. Disaggregated memory for expansion and sharing in blade servers. *ACM SIGARCH computer architecture news* 37, 3 (2009), 267–278.

[42] Kevin Lim, Yoshio Turner, Jose Renato Santos, Alvin AuYoung, Jichuan Chang, Parthasarathy Ranganathan, and Thomas F Wenisch. 2012. System-level implications of disaggregated memory. In *IEEE International Symposium on High-Performance Comp Architecture*. IEEE, 1–12.

[43] Rui Lin, Yuxin Cheng, Marilet De Andrade, Lena Wosinska, and Jiajia Chen. 2020. Disaggregated data centers: Challenges and trade-offs. *IEEE Communications Magazine* 58, 2 (2020), 20–26.

[44] Sergio Maffeis, John C Mitchell, and Ankur Taly. 2010. Object capabilities and isolation of untrusted web applications. In *2010 IEEE Symposium on Security and Privacy*. IEEE, 125–140.

[45] Kshiteej Mahajan, Arjun Balasubramanian, Arjun Singhvi, Shivaram Venkataraman, Aditya Akella, Amar Phanishayee, and Shuchi Chawla. 2020. Themis: Fair and efficient GPU cluster scheduling. In *17th USENIX Symposium on Networked Systems Design and Implementation*.

[46] Mark S Miller, Ka-Ping Yee, Jonathan Shapiro, et al. 2003. *Capability myths demolished*. Technical Report. Technical Report SRL2003-02, Johns Hopkins University Systems Research ....

[47] Jaehong Min, Ming Liu, Tapan Chugh, Chenxingyu Zhao, Andrew Wei, In Hwan Doh, and Arvind Krishnamurthy. 2021. Gimbal: enabling multi-tenant storage

disaggregation on SmartNIC JBOFs. In *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*. 106–122.

[48] Dave Minturn. 2015. Nvm express over fabrics. In *11th Annual OpenFabrics International OFS Developers' Workshop*.

[49] Jayadev Misra and K. Mani Chandy. 1981. Proofs of networks of processes. *IEEE transactions on software engineering* 4 (1981), 417–426.

[50] Sape J. Mullender, Guido Van Rossum, AS Tananbaum, Robbert Van Renesse, and Hans Van Staveren. 1990. Amoeba: A distributed operating system for the 1990s. *Computer* 23, 5 (1990), 44–53.

[51] Mihir Nanavati, Jake Wires, and Andrew Warfield. 2017. Decibel: Isolation and Sharing in Disaggregated Rack-Scale Storage.. In *NSDI, Volume 17*. 17–33.

[52] Roger M Needham and Robin DH Walker. 1977. The Cambridge CAP computer and its protection system. *ACM SIGOPS Operating Systems Review* 11, 5 (1977), 1–10.

[53] Richard Otter. 1948. The number of trees. *Annals of Mathematics* (1948), 583–599.

[54] Antonios D Papaioannou, Reza Nejabati, and Dimitra Simeonidou. 2016. The benefits of a disaggregated data centre: A resource allocation approach. In *2016 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 1–7.

[55] Christian Pinto, Dimitris Syrivelis, Michele Gazzetti, Panos Koutsovasilis, Andrea Reale, Kostas Katrinis, and H Peter Hofstee. 2020. Thymesisflow: A software-defined, hw/sw co-designed interconnect stack for rack-scale memory disaggregation. In *2020 53rd Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*. IEEE, 868–880.

[56] Andrew Putnam, Adrian M Caulfield, Eric S Chung, Derek Chiou, Kypros Constantinides, John Demme, Hadi Esmaeilzadeh, Jeremy Fowers, Gopi Prashanth Gopal, Jan Gray, et al. 2014. A reconfigurable fabric for accelerating large-scale datacenter services. *ACM SIGARCH Computer Architecture News* 42, 3 (2014), 13–24.

[57] Richard F Rashid and George G Robertson. 1981. Accent: A communication oriented network operating system kernel. *ACM SIGOPS Operating Systems Review* 15, 5 (1981), 64–75.

[58] Marc Rozier, Vadim Abrossimov, François Armand, Ivan Boule, Michel Gien, Marc Guillemont, Frédéric Herrmann, Claude Kaiser, Sylvain Langlois, Pierre Léonard, et al. 1992. Overview of the Chorus distributed operating system. In *Workshop on Micro-Kernels and Other Kernel Architectures*. Seattle WA (USA), 39–70.

[59] Jerome H Saltzer. 1974. Protection and the control of information sharing in Multics. *Commun. ACM* 17, 7 (1974), 388–402.

[60] Jonathan S Shapiro, Jonathan M Smith, and David J Farber. 1999. EROS: a fast capability system. In *Proceedings of the seventeenth ACM symposium on Operating systems principles*. 170–185.

[61] Vishal Shrivastav, Asaf Valadarsky, Hitesh Ballani, Paolo Costa, Ki Suh Lee, Han Wang, Rachit Agarwal, and Hakim Weatherspoon. 2019. Shoal: A Network Architecture for Disaggregated Racks.. In *NSDI*. 255–270.

[62] Richard J Swan, Samuel H Fuller, and Daniel P Siewiorek. 1977. Cm* a modular, multi-microprocessor. In *Proceedings of the June 13-16, 1977, national computer conference*. 637–644.

[63] Shin-Yeh Tsai and Yiying Zhang. 2019. A double-edged sword: security threats and opportunities in one-sided network communication. In *Proceedings of the 11th USENIX Conference on Hot Topics in Cloud Computing*. 3–3.

[64] Jacob Wahlgren, Maya Gokhale, and Ivy B Peng. 2022. Evaluating Emerging CXL-enabled Memory Pooling for HPC Systems. *arXiv preprint arXiv:2211.02682* (2022).

[65] Chenxi Wang, Haoran Ma, Shi Liu, Yuanqi Li, Zhenyuan Ruan, Khanh Nguyen, Michael D Bond, Ravi Netravali, Miryung Kim, and Guoqing Harry Xu. 2020. Semeru: A memory-disaggregated managed runtime. In *Proceedings of the 14th USENIX Conference on Operating Systems Design and Implementation*. 261–280.

[66] Jonathan Woodruff, Robert NM Watson, David Chisnall, Simon W Moore, Jonathan Anderson, Brooks Davis, Ben Laurie, Peter G Neumann, Robert Norton, and Michael Roe. 2014. The CHERI capability model: Revisiting RISC in an age of risk. In *2014 ACM/IEEE 41st International Symposium on Computer Architecture (ISCA)*. IEEE, 457–468.

[67] William Wulf, Ellis Cohen, William Corwin, Anita Jones, Roy Levin, Charles Pierson, and Fred Pollack. 1974. Hydra: The kernel of a multiprocessor operating system. *Commun. ACM* 17, 6 (1974), 337–345.