

Copyright 2020 Carnegie Mellon University and Hyoseung Kim.

This material is based upon work funded and supported by the Department of Defense under No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other official documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH REGARD TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

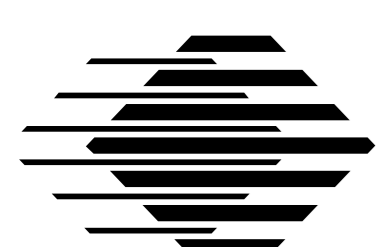
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

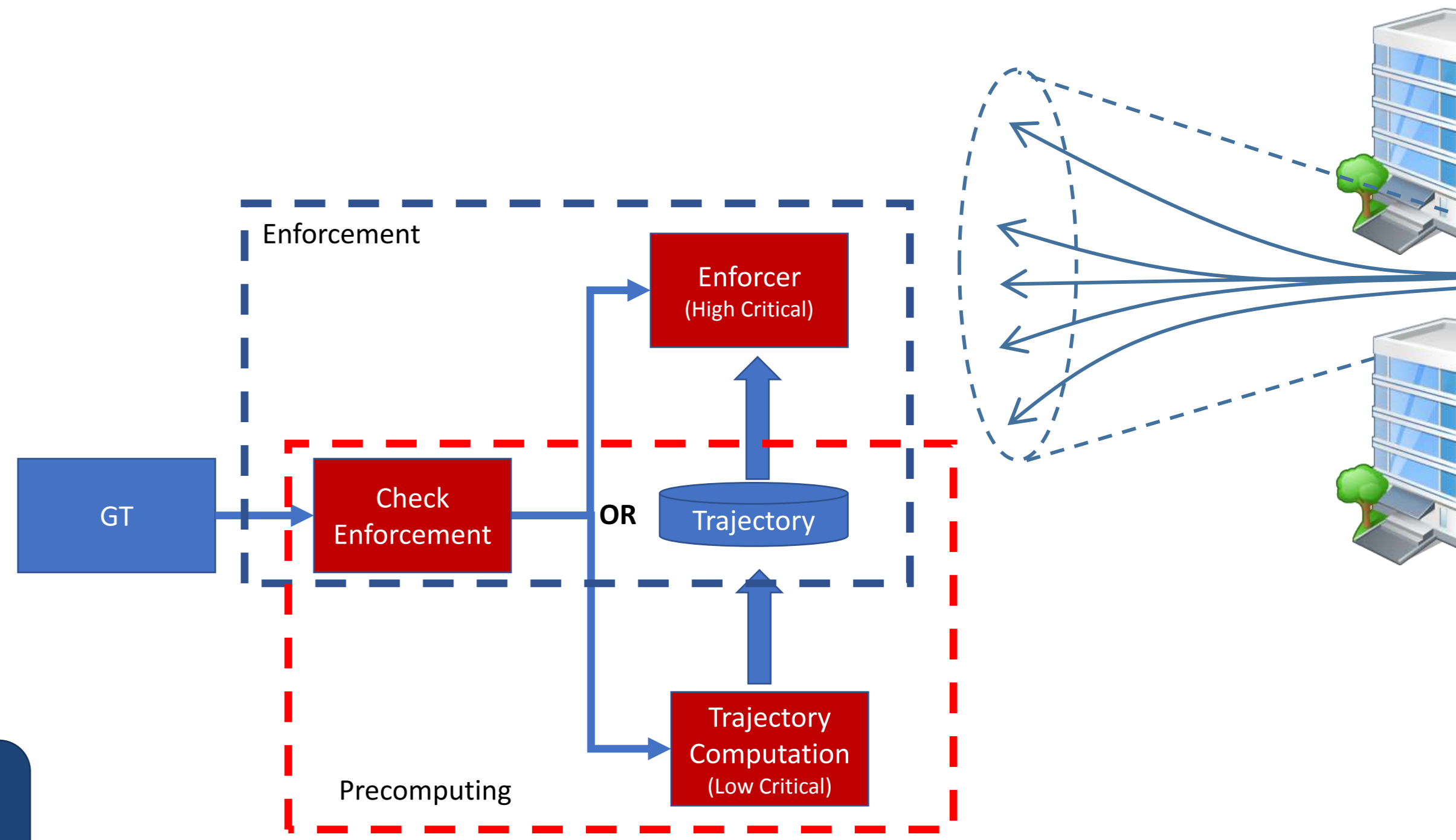
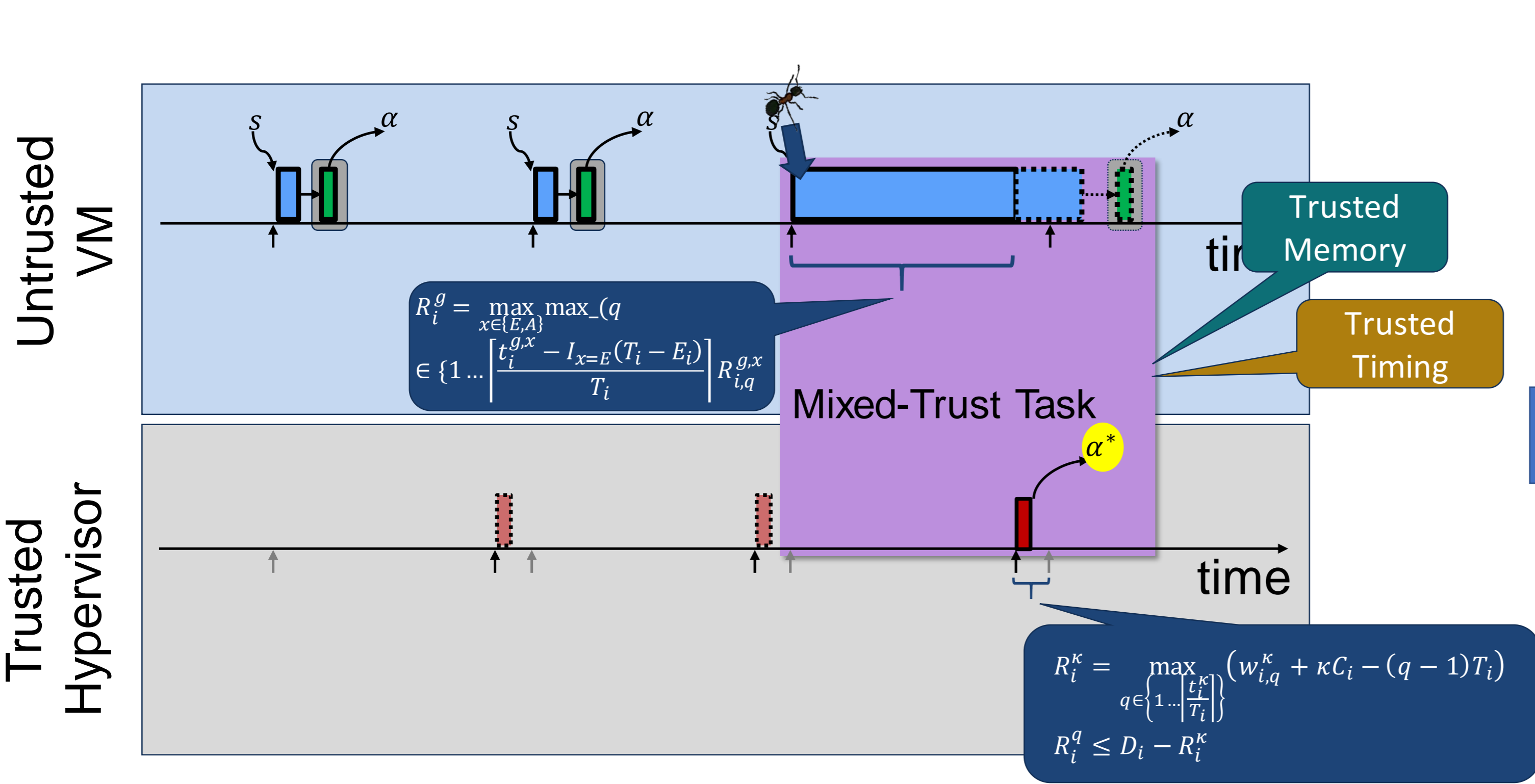
Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

Carnegie Mellon[®] is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University. DM20-1076





Mixed Trust Scheduling Combines (in mixed-trust task)

- Untrusted part (Guesttask - GT) in VM (preemptive FP)
- Trusted part (Hypertask - HT) in verified HV (non-preemptive FP)
- to monitor and enforce safety properties (w trusted timing)

Enforcement may need to look ahead (trajectory)
Precomputing reuses time unused by HT

- To pre-plan enforcement (e.g., trajectories)

Based on multi-frame scheduling:

- Response time sketch: $R_i^p = \kappa C_i^p + \sum \left\lfloor \frac{R_i^p}{T_j} \right\rfloor \kappa C_j^p - \left\lfloor \frac{R_i^p}{I_j T_j} \right\rfloor (\kappa C_j^p - \kappa C_j^e)$
 - With: WCET predictive: κC_i^p , WCET enforcer κC_j^e , Ratio of predictive to enforcer I_j
- Non-preemptive
 - Enforcement
 - Prediction

$$R_i^{\kappa,e} = \max_{q \in \{1 \dots \lfloor \frac{t_i^{\kappa}}{T_i} \rfloor\}} (w_{i,q}^{\kappa} + \kappa C_i^m - (q-1)T_i),$$

$$t_i^{g,x} = \left(\sum_{j \in L_i} \text{rbf}_j^E(t_i^{g,x}, 0) \right) + \text{rbf}_i^x(t_i^{g,x}, 1) + \sum_{j \in H_i} \max_{y \in \{E, A\}} \text{rbf}_j^y(t_i^{g,x}, 1),$$

$$w_{i,q}^{g,x} = \left(\sum_{j \in L_i} \text{rbf}_j^E(w_{i,q}^{g,x}, 0) \right) + qC_i + (q-1 + \mathcal{B}_{(x=E)})\kappa C_i + \sum_{j \in H_i} \max_{y \in \{E, A\}} \text{rbf}_j^y(w_{i,q}^{g,x}, 1).$$

$$t_i^{\kappa,p} = \max_{j \in \kappa L_i} \kappa C_j^m + \left\lfloor \frac{t_i^{\kappa,p}}{T_i} \right\rfloor \kappa C_i^p + CP(i, t_i^{\kappa,p}) + \sum_{j \in \kappa H_i} \left(\left\lfloor \frac{t_i^{\kappa,p}}{T_j} \right\rfloor \kappa C_j^p + CP(j, t_i^{\kappa,p}) \right),$$

$$w_{i,q}^{\kappa,p} = \max_{j \in \kappa L_i} \kappa C_j^m + (q-1)\kappa C_i^p + Q(i, q-1) + \sum_{j \in \kappa H_i} \left(\left(\left\lfloor \frac{w_{i,q}^{\kappa,p}}{T_j} \right\rfloor + 1 \right) \kappa C_j^p + CP_w(j, w_{i,q}^{\kappa,p}) \right),$$

$$CP(j, t_i^{\kappa,p}) = \begin{cases} \left\lfloor \frac{t_i^{\kappa,p}}{T_j \cdot I_j} \right\rfloor (\kappa C_j^e - \kappa C_j^p) \\ - \left\lfloor \frac{t_i^{\kappa,p}}{T_j \cdot I_j} \right\rfloor (\kappa C_j^p - \kappa C_j^e) \end{cases}$$

$$Q(i, q) = \begin{cases} \left\lfloor \frac{q}{I_i} \right\rfloor (\kappa C_i^e - \kappa C_i^p) \\ - \left\lfloor \frac{q}{I_i} \right\rfloor (\kappa C_i^p - \kappa C_i^e) \end{cases}$$

$$CP_w(j, w_{i,q}^{\kappa,p}) = \begin{cases} \left(\left\lfloor \frac{w_{i,q}^{\kappa,p}}{T_j \cdot I_j} \right\rfloor + 1 \right) (\kappa C_j^e - \kappa C_j^p) \\ - \left\lfloor \frac{w_{i,q}^{\kappa,p}}{T_j \cdot I_j} \right\rfloor (\kappa C_j^p - \kappa C_j^e) \end{cases}$$

