Performance-sensitive Real-time Risk Management is NP-Hard

By: Ashish Gehani

Department of Computer Science, Duke University

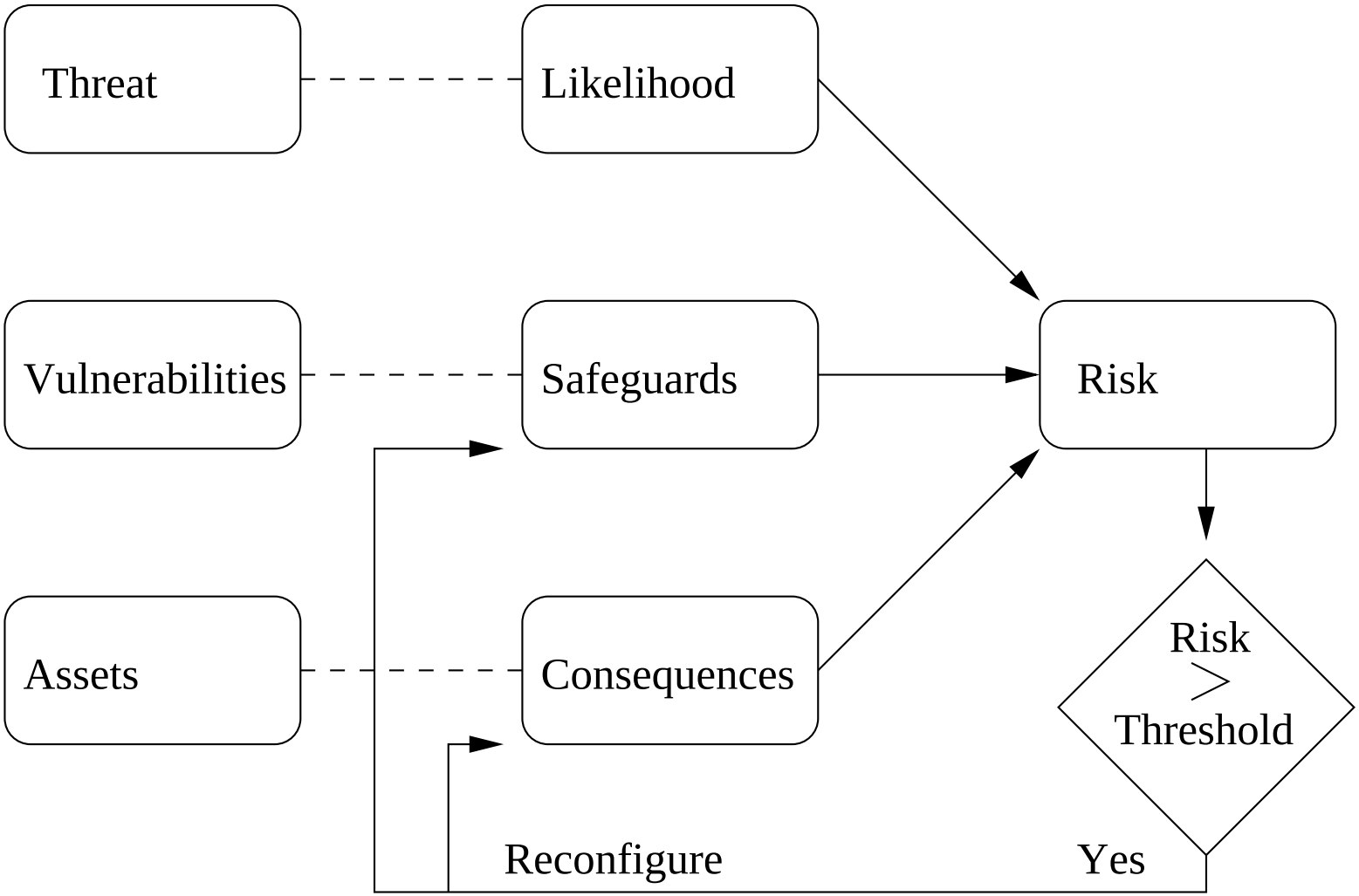
PROBLEM : Intrusion response

- Manual response decreasingly tenable:
  - High attack frequency
  - Great attack diversity
  - Rapid attack execution
  - Protection Time < Detection Time + Response Time
- False positives preclude retaliation
- Network connections encrypted

SOLUTION STRATEGY

- Automate response:
  - Model runtime risk
  - Build risk management primitives
  - Dynamically manage risk
  - Minimize impact on performance
- Passive response - limit to owner's domain
- Host-based

RISK MODEL : Management



RISK MODEL : Threat

- Events : $E \stackrel{\prec}{=} \{e_1, e_2, \ldots\}$
- Threats : $T = \{t_1, t_2, \ldots\}$
- Signature : $S(t_\alpha) \stackrel{\prec}{=} \{s_1, s_2, \ldots\}, \quad s_i \in E, \quad t_\alpha \in T$
- Likelihood : $\mathcal{T}(t_\alpha) = \mu(t_\alpha, E \stackrel{\prec}{\cap} S(t_\alpha)), \quad t_\alpha \in T$

RISK MODEL : Vulnerability

- Weaknesses : $W = \{w_1, w_2, \ldots\}, \quad W(t_\alpha) \subseteq W, \quad t_\alpha \in T$
- Permissions : $P = \{p_1, p_2, \ldots\}, \quad P(w_\gamma) \subseteq P, \quad w_\gamma \in W$
- Safeguards : $\hat{P}(t_\alpha) = \bigcup_{w_\gamma \in W(t_\alpha)} P(w_\gamma), \quad t_\alpha \in T$
- Static Exposure: $v(p_\lambda) \in \{0, 1\}, \quad p_\lambda \in P$
- Dynamic Exposure: $v'(p_\lambda) \in [0, 1], \quad p_\lambda \in P$
- Vulnerability : $\mathcal{V}(t_\alpha) = \sum_{p_\lambda \in \hat{P}(t_\alpha)} \frac{v(p_\lambda) \times v'(p_\lambda)}{|\hat{P}(t_\alpha)|}, \quad t_\alpha \in T$

RISK MODEL : Consequence

- Objects : $O = \{o_1, o_2, \ldots\}$
- Assets : $A(t_\alpha) \subseteq O$
- Confidentiality : $c(o_\beta), \quad o_\beta \in O$
- Integrity : $i(o_\beta), \quad o_\beta \in O$
- Availability : $a(o_\beta), \quad o_\beta \in O$
- Consequence : $\mathcal{C}(t_\alpha) = \sum_{o_\beta \in A(t_\alpha)} c(o_\beta) + i(o_\beta) + a(o_\beta), \quad t_\alpha \in T$

RISK MODEL : Unmanaged Risk

- Unmanaged Risk : $\mathcal{R} = \sum_{t_\alpha \in T} \mathcal{T}(t_\alpha) \times \mathcal{V}(t_\alpha) \times \mathcal{C}(t_\alpha)$
- Computation Time : $O(|T| \times |P| \times |O|)$

RISK MODEL : Risk Management Primitives

- Auxiliary safeguards : $\Psi(P) \subseteq P$
- Static checks : $\Omega(P) \subseteq P$
- $\Psi(P) \cap \Omega(P) = \phi, \quad \Psi(P) \cup \Omega(P) = P$
- Curtailed consequences : $\Psi(O) \subseteq O$
- Transparent access : $\Omega(O) \subseteq O$
- $\Psi(O) \cap \Omega(O) = \phi, \quad \Psi(O) \cup \Omega(O) = O$

RISK MODEL : Managed Risk

- Managed Vulnerability : $\mathcal{V}'(t_\alpha) =$

$$\sum_{p_\lambda \in \hat{P}(t_\alpha) \cap \Omega(P)} \frac{v(p_\lambda)}{|\hat{P}(t_\alpha)|} + \sum_{p_\lambda \in \hat{P}(t_\alpha) \cap \Psi(P)} \frac{v(p_\lambda) \times v'(p_\lambda)}{|\hat{P}(t_\alpha)|}, \quad t_\alpha \in T$$

- Managed Consequence :

$$\mathcal{C}'(t_\alpha) = \sum_{o_\beta \in A(t_\alpha) \cap \Omega(O)} c(o_\beta) + i(o_\beta) + a(o_\beta), \quad t_\alpha \in T$$

- Managed Risk : $\mathcal{R}' = \sum_{t_\alpha \in T} \mathcal{T}(t_\alpha) \times \mathcal{V}'(t_\alpha) \times \mathcal{C}'(t_\alpha)$

RISK MODEL : Risk Tolerance

- Event : e
- Risk before : $\mathcal{R}_b$
- Risk change : $\epsilon \neq 0$
- Risk after : $\mathcal{R}_a = \mathcal{R}_b + \epsilon$
- Risk threshold : $\mathcal{R}_0$
- $\epsilon > 0 \quad \wedge \quad \mathcal{R}_a > \mathcal{R}_0 \quad \Rightarrow \quad Reduce()$
- $\epsilon > 0 \quad \wedge \quad \mathcal{R}_a \leq \mathcal{R}_0 \quad \Rightarrow \quad \phi$
- $\epsilon < 0 \quad \Rightarrow \quad \mathcal{R}_a = \mathcal{R}_b + \epsilon < \mathcal{R}_b < \mathcal{R}_0 \quad \Rightarrow \quad Relax()$

RISK MODEL : Risk Recalculation

- Threat change :

  $\delta(\mathcal{T}(t_\alpha), e) \quad = \quad \mu(t_\alpha, (E \cup e) \overset{\prec}{\cap} S(t_\alpha)) - \mu(t_\alpha, E \overset{\prec}{\cap} S(t_\alpha))$

- Threats affected :

  $\Delta(T, e) \quad : \quad \delta(\mathcal{T}(t_\alpha), e) \neq 0 \quad \Rightarrow \quad t_\alpha \in \Delta(T, e)$

- Update cost : $O(|T|) \quad \because \quad \mathcal{V}'(t_\alpha), \mathcal{C}'(t_\alpha)$ cached

RISK MODEL : Risk Reduction

- Enable safeguards : $\rho(\Omega(P)) \subseteq \Omega(P)$
- Enable curtailments : $\rho(\Omega(O)) \subseteq \Omega(O)$
- Find : $\rho(\Omega(P)), \rho(\Omega(O)) \quad \Rightarrow \quad \mathcal{R}'' < \mathcal{R}_0$
- Reduced Vulnerability :

$$\mathcal{V}''(t_\alpha) = \sum_{p_\lambda \in (\hat{P}(t_\alpha) \cap \Omega(P) - \rho(\Omega(P)))} \frac{v(p_\lambda)}{|\hat{P}(t_\alpha)|} + \sum_{p_\lambda \in (\hat{P}(t_\alpha) \cap \Psi(P) \cup \rho(\Omega(P)))} \frac{v(p_\lambda) \times v'(p_\lambda)}{|\hat{P}(t_\alpha)|}$$

- Reduced Consequence :

$$\mathcal{C}''(t_\alpha) = \sum_{o_\beta \in (A(t_\alpha) \cap \Omega(O) - \rho(\Omega(O)))} c(o_\beta) + i(o_\beta) + a(o_\beta)$$

- Reduced Risk : $\mathcal{R}'' = \sum_{t_\alpha \in T} \mathcal{T}(t_\alpha) \times \mathcal{V}''(t_\alpha) \times \mathcal{C}''(t_\alpha)$

RISK MODEL : Risk Relaxation

- Disable safeguards : $\rho(\Psi(P)) \subseteq \Psi(P)$
- Disable curtailments : $\rho(\Psi(O)) \subseteq \Psi(O)$
- Find : $\rho(\Psi(P)), \rho(\Psi(O)) \quad \Rightarrow \quad \mathcal{R}'' < \mathcal{R}_0$
- Relaxed Vulnerability :

$$\mathcal{V}''(t_\alpha) = \sum_{p_\lambda \in (\hat{P}(t_\alpha) \cap \Omega(P) \cup \rho(\Psi(P)))} \frac{v(p_\lambda)}{|\hat{P}(t_\alpha)|} + \sum_{p_\lambda \in (\hat{P}(t_\alpha) \cap \Psi(P) - \rho(\Psi(P)))} \frac{v(p_\lambda) \times v'(p_\lambda)}{|\hat{P}(t_\alpha)|}$$

- Reduced Consequence :

$$\mathcal{C}''(t_\alpha) = \sum_{o_\beta \in (A(t_\alpha) \cap \Omega(O) \cup \rho(\Psi(O)))} c(o_\beta) + i(o_\beta) + a(o_\beta)$$

- Reduced Risk : $\mathcal{R}'' = \sum_{t_\alpha \in T} \mathcal{T}(t_\alpha) \times \mathcal{V}''(t_\alpha) \times \mathcal{C}''(t_\alpha)$

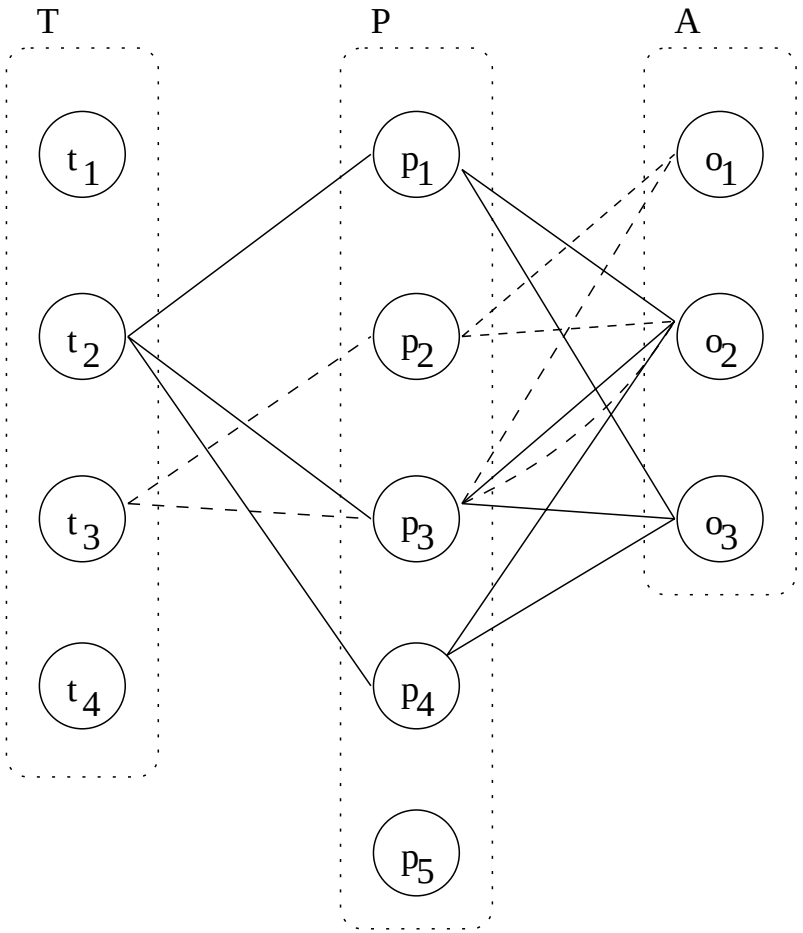
RISK MODEL : Constraints

- Increase of Risk Reduction Cost :
  $$\zeta(\rho(\Omega(P)), \rho(\Omega(O))) = \sum_{p_\lambda \in \rho(\Omega(P))} f(p_\lambda) + \sum_{o_\beta \in \rho(\Omega(O))} f(o_\beta)$$
- Decrease of Risk Relaxation Cost :
  $$\zeta(\rho(\Psi(P)), \rho(\Psi(O))) = \sum_{p_\lambda \in \rho(\Psi(P))} f(p_\lambda) + \sum_{o_\beta \in \rho(\Psi(O))} f(o_\beta)$$
- Risk Reduction : $\min \zeta(\rho(\Omega(P)), \rho(\Omega(O))), \quad \mathcal{R}'' \leq \mathcal{R}_0$
- Risk Relaxation : $\max \zeta(\rho(\Psi(P)), \rho(\Psi(O))), \quad \mathcal{R}'' \leq \mathcal{R}_0$

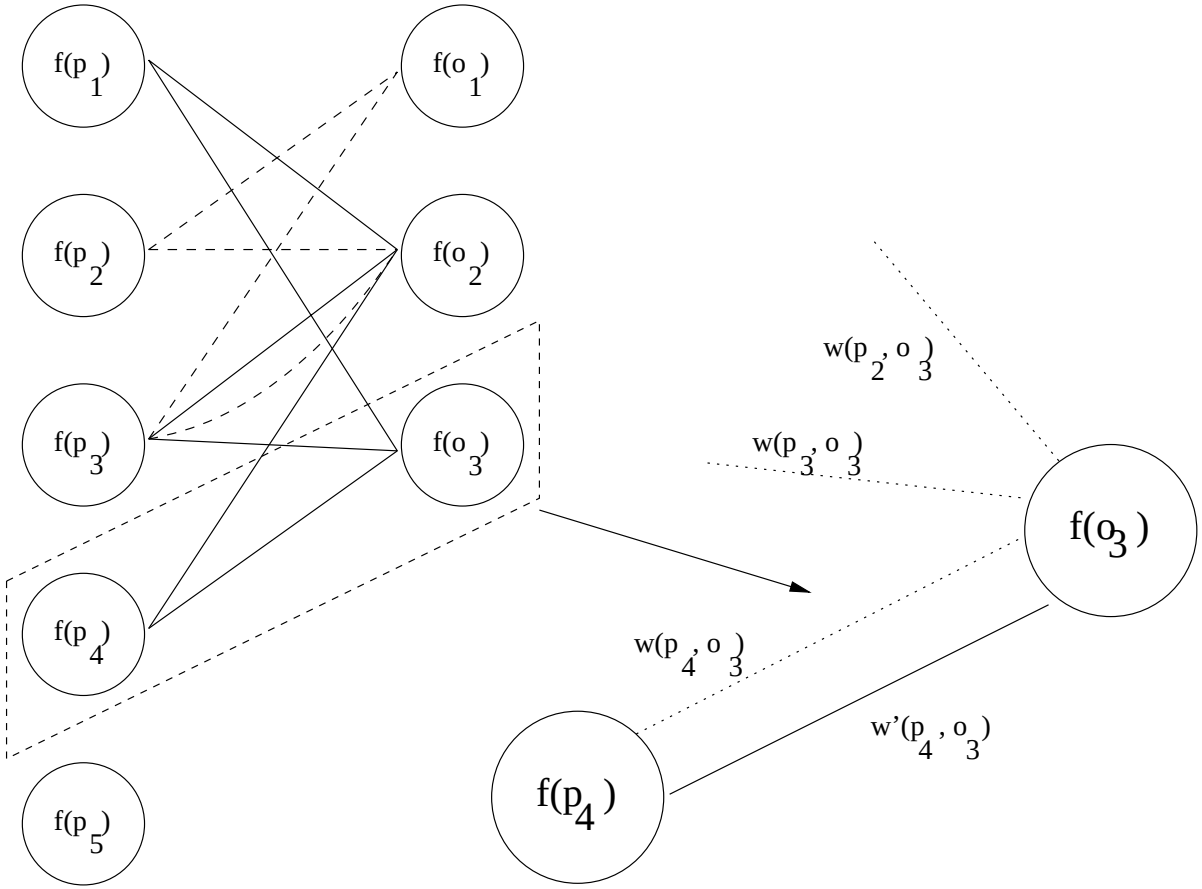
RISK MODEL : Time Complexity

- Choices of $\rho(\Omega(P)), \rho(\Omega(O))$
  for Risk Reduction : $O(2^{(|P|+|O|)})$
- Choices of $\rho(\Psi(P)), \rho(\Psi(O))$
  for Risk Relaxation : $O(2^{(|P|+|O|)})$
- Linear Objective Function :
  for Risk Reduction : $\min \zeta(\rho(\Omega(P)), \rho(\Omega(O)))$
  for Risk Relaxation : $\max \zeta(\rho(\Psi(P)), \rho(\Psi(O)))$
- Quadratic Constraint : $\mathcal{R}'' \leq \mathcal{R}_0$

COMPLEXITY : Risk Graph



COMPLEXITY : Response Graph



COMPLEXITY : Response Graph Properties

- Bipartite graph, Partitions : P, O
- Vertex weights : $f(p_\lambda)$, $f(o_\beta)$
- Safeguard dependent edge weights : $w'(p_\lambda, o_\beta) =$

$$\sum_{t_\alpha \in T : p_\lambda \in \hat{P}(t_\alpha) \wedge o_\beta \in A(t_\alpha)} \mathcal{T}(t_\alpha) \times \frac{v(p_\lambda) \times 1 - v'(p_\lambda)}{|\hat{P}(t_\alpha)|} \times c(o_\beta) + i(o_\beta) + a(o_\beta)$$

- Consequence dependent edge weights : $w(p_\lambda, o_\beta) =$

$$\sum_{t_\alpha \in T : p_\lambda \in \hat{P}(t_\alpha) \wedge o_\beta \in A(t_\alpha)} \mathcal{T}(t_\alpha) \times \frac{v(p_\lambda) \times v'(p_\lambda)}{|\hat{P}(t_\alpha)|} \times c(o_\beta) + i(o_\beta) + a(o_\beta)$$

COMPLEXITY : Optimization Problem

- Risk reduction
- Select vertex set : $\rho(\Omega(P)), \rho(\Omega(O))$
  - Minimize $\sum_{p_\lambda \in \rho(\Omega(P))} f(p_\lambda) + \sum_{o_\beta \in \rho(\Omega(O))} f(o_\beta)$
  - Constrained by : $W_e \geq R_a - R_0$

    $W_e =$

    $$\sum_{p_\lambda \in \rho(\Omega(P)), o_\beta \in \rho(\Omega(O))} w'(p_\lambda, o_\beta) \quad + \sum_{p_\lambda \in P - \rho(\Omega(P)), o_\beta \in \rho(O)} w(p_\lambda, o_\beta)$$

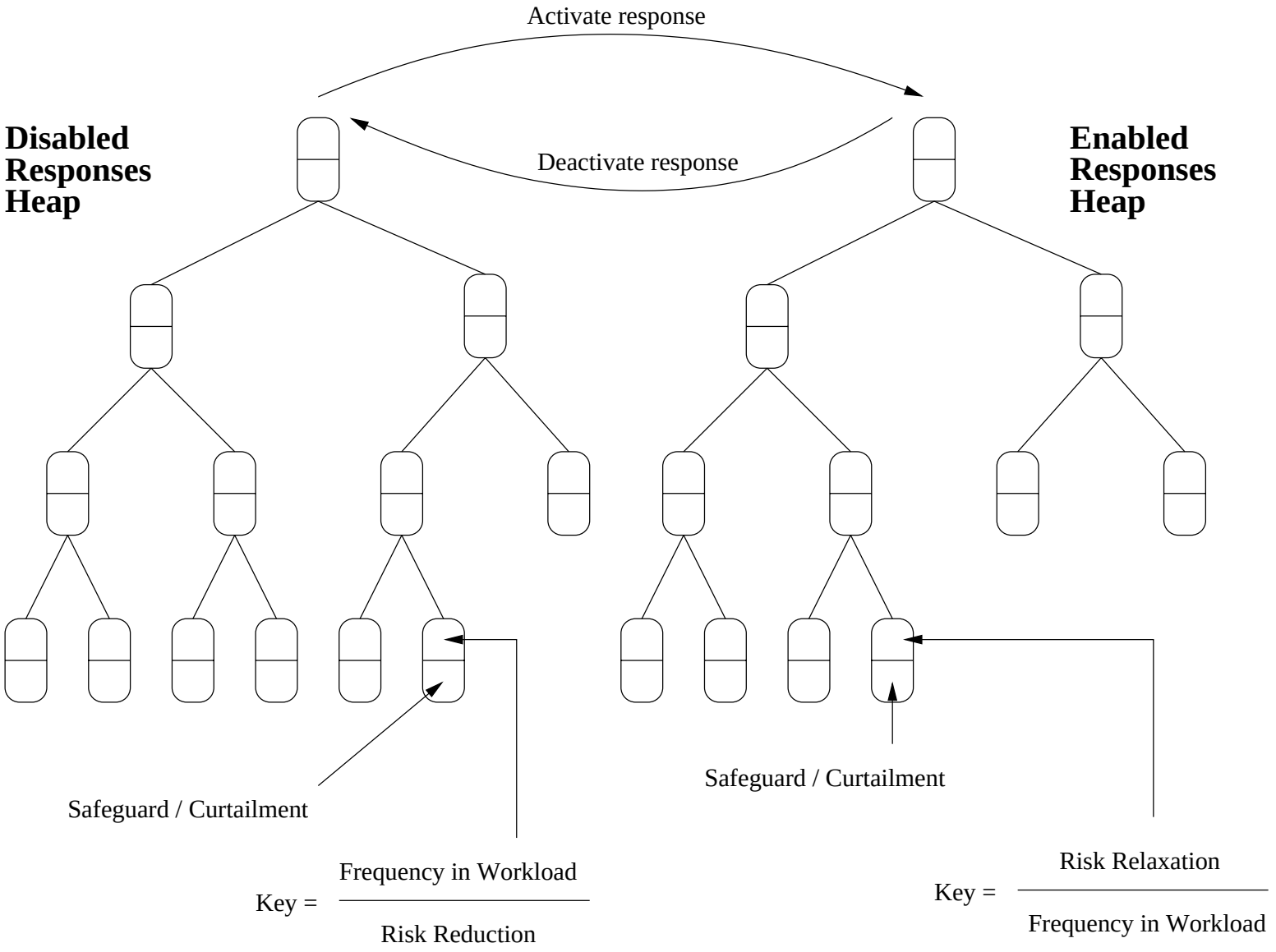
COMPLEXITY : Decision Problem

- Input:
  - Bipartite response graph
  - Minimum for sum of edge weights
  - Target sum of vertex weights
- Output $true$ if solution found, else $false$

COMPLEXITY : NP-Hard

- Reduce to Maximum Edge Biclique
- Construction:
  - $\forall p_\lambda, \quad f(p_\lambda) = 1$
  - $\forall o_\beta, \quad f(o_\beta) = 1$
  - $\forall p_\lambda \forall o_\beta, \quad w(p_\lambda, o_\beta) = 0$
  - $\forall p_\lambda \forall o_\beta, \quad w'(p_\lambda, o_\beta) = 1$
- Find solution with Risk Reduction Algorithm
- Given vertex count, biclique has maximum edge count
- Solves Maximum Edge Biclique

HEURISTIC : Response Heaps



HEURISTIC : Pre-Processing

Step 1 $\forall p_\lambda \in \Omega(P)$, calculate Benefit-to-Cost ratio:

$$\kappa(p_\lambda) = \frac{\displaystyle\sum_{t_\alpha : p_\lambda \in (\hat{P}(t_\alpha) \cap \Omega(P))} \mathcal{T}(t_\alpha) \times \frac{v(p_\lambda) \times (1 - v'(p_\lambda))}{|\hat{P}(t_\alpha)|} \times \mathcal{C}'(t_\alpha)}{f(p_\lambda)}$$

Step 2 $\forall o_\beta \in \Omega(O)$, calculate Benefit-to-Cost ratio:

$$\kappa(o_\beta) = \frac{c(o_\beta) + i(o_\beta + a(o_\beta)) \quad \times \displaystyle\sum_{t_\alpha : o_\beta \in (A(t_\alpha) \cap \Omega(O))} \mathcal{T}(t_\alpha) \times \mathcal{V}'(t_\alpha)}{f(o_\beta)}$$

HEURISTIC : Primitive Selection

Step 3 Set $\rho(\Omega(P)) = \rho(\Omega(O)) = \phi$

Step 4 Choose: $r = \max\ p_{max}, o_{max}$ where:

$p_{max} = \max\ \kappa(p_\lambda), \quad p_\lambda \in \Omega(P)$

$o_{max} = \max\ \kappa(o_\beta), \quad o_\beta \in \Omega(O)$

Add r to: $\rho(\Omega(P))$ / $\rho(\Omega(O))$

Step 5

$$r = p_\lambda \quad \Rightarrow \quad \forall o_\beta \in \bigcup_{t_\alpha : p_\lambda \in \hat{P}(t_\alpha)} A(t_\alpha) \quad : \text{Update } \kappa(o_\beta)$$

$$r = o_\beta \quad \Rightarrow \quad \forall p_\lambda \in \bigcup_{t_\alpha : o_\beta \in A(t_\alpha)} \hat{P}(t_\alpha) \quad : \text{Update } \kappa(p_\lambda)$$

Step 6 Recalculate Risk :

$$\mathcal{R}'' = \mathcal{R}_a \quad - \sum_{p_\lambda \in \rho(\Omega(P))} \kappa(p_\lambda) \times f(p_\lambda) \quad - \sum_{o_\beta \in \rho(\Omega(O))} \kappa(o_\beta) \times f(o_\beta)$$

HEURISTIC : Response Completion

Step 7

$\mathcal{R}'' > \mathcal{R}_0 \quad \Rightarrow \quad$ Step 4

$\mathcal{R}'' \leq \mathcal{R}_0 \quad \Rightarrow \quad$ Utilize Response : $\rho(\Omega(P)), \rho(\Omega(O))$

- Time Complexity :
  $O((\rho(\Omega(P)) + \rho(\Omega(O))) \times (\log|P| + \log|O| + \sum_{t_\alpha \in T} (|\hat{P}(t_\alpha)| + |A(t_\alpha)|)))$
- Worst Case : $O(|P| + |O|)^2$
- Response Initiation Time : $O(1)$