Attack-Aware Cyber Insurance of Interdependent Computer Networks

Rui Zhang Quanyan Zhu

Department of Electrical and Computer Engineering

Tandon School of Engineering

New York University

June 27

Motivations

Cyber-attacks are threats to network security.

- Data Breaches;
- Financial Losses;
- Disruption of Services.

Network security becomes more challenging.

1. Attackers become more stealthy and sophisticated.
2. Networks become more complex.

Defense mechanisms cannot guarantee perfect network security.

- Firewalls;
- Intrusion Detection Systems;
- Moving Target Defenses.

Motivations

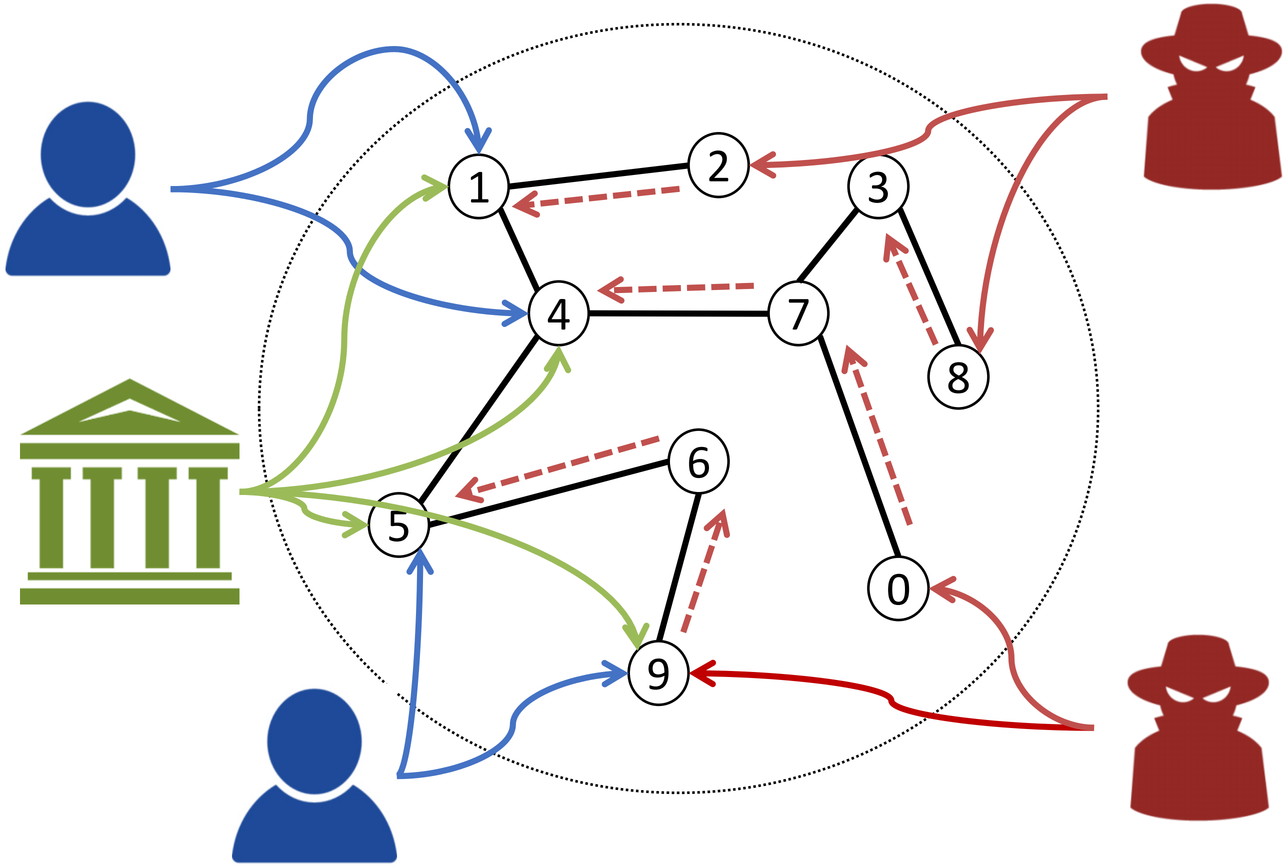
Cyber insurance provides network users a valuable additional layer of protection to mitigate potential vulnerabilities [Kesan et al., 2005] [Bolot et al., 2009] [Pal et al., 2014].

Different from the traditional insurance paradigm, cyber insurance has two unique features.

1. The risks of cyber-attacks are not created by natural failures but by intelligent attackers who deliberately inflict damages on the network.
2. Cyber risks can propagate over a network.

We establish a bi-level game-theoretic model to capture the complex interactions among different types of players, and we further extend it to study a network of users and their risk interdependencies.

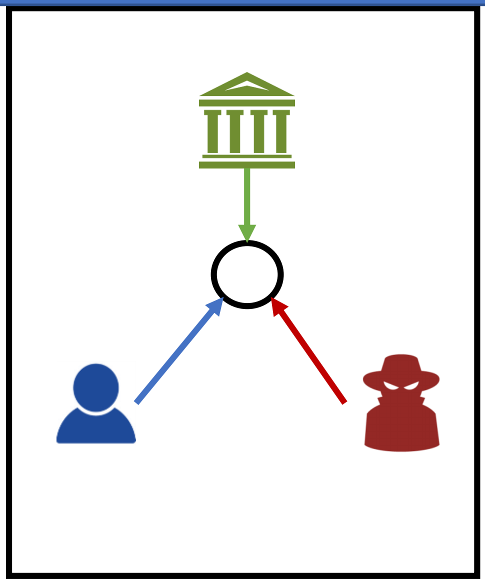
Problem Statement: Overview



- Network: Well-Connected; No Isolated Node.
- Users: Protect themselves by local protection methods and mitigate the losses from cyber attacks by subscribing to cyber insurance.
- Attackers: Conduct cyber-attacks to achieve malicious goals.
- Insurers: Provide cyber insurance.

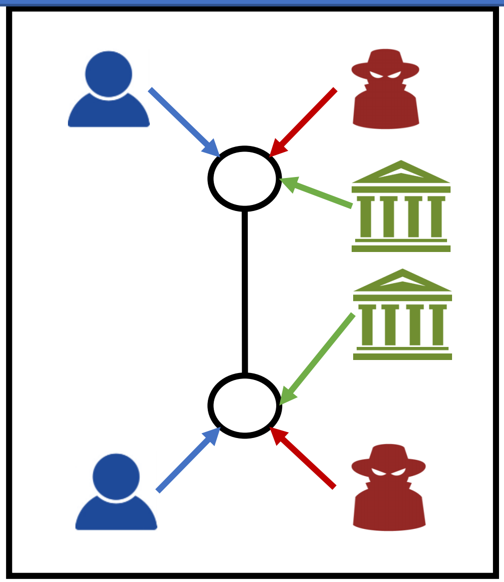
Problem Statement: Cases

Case 1



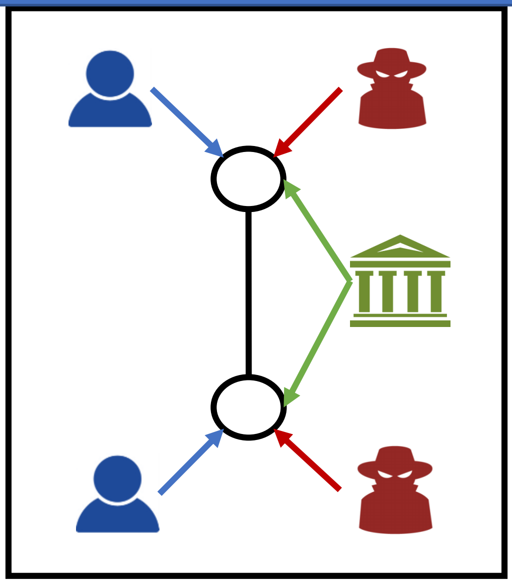
- 1 Node
- 1 User
- 1 Attacker
- 1 Insurer

Case 2(a)



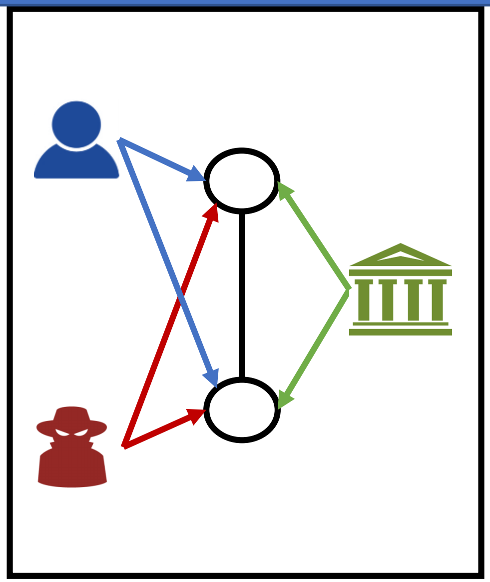
- N Nodes
- N Users
- N Attackers
- N Insurers

Case 2(b)



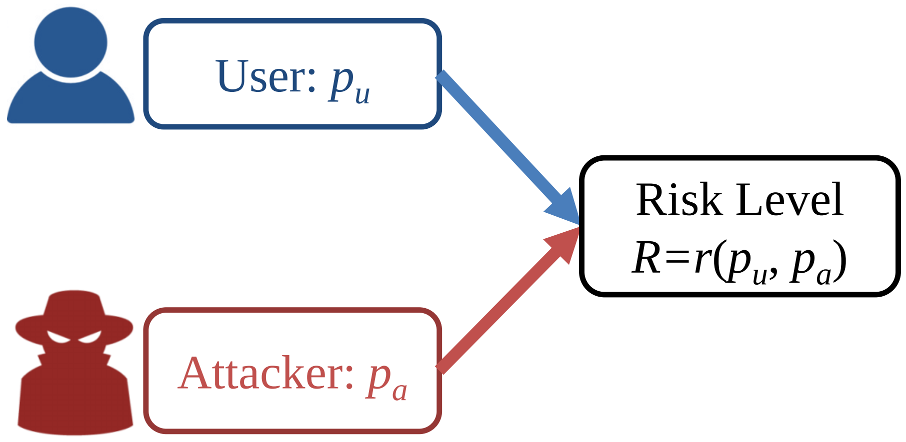
- N Nodes
- N Users
- N Attackers
- 1 Insurer

Case 3

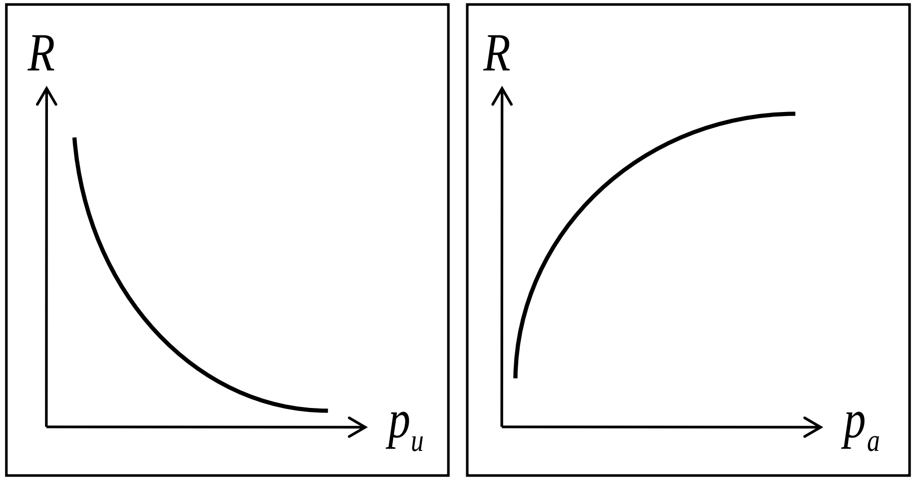


- N Nodes
- 1 User
- 1 Attacker
- 1 Insurer

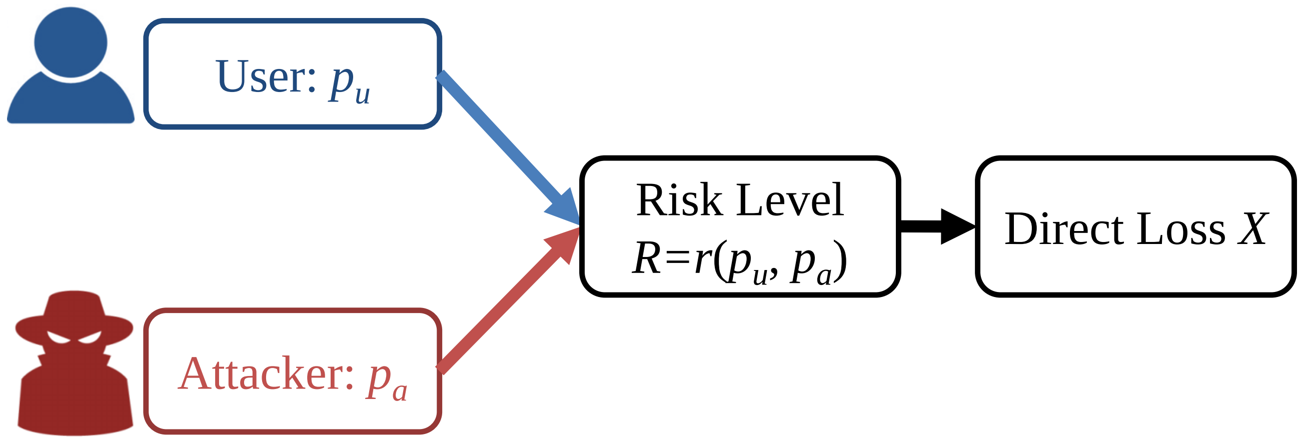
Case 1: 1 Node-1 User-1 Attacker-1 Insurer



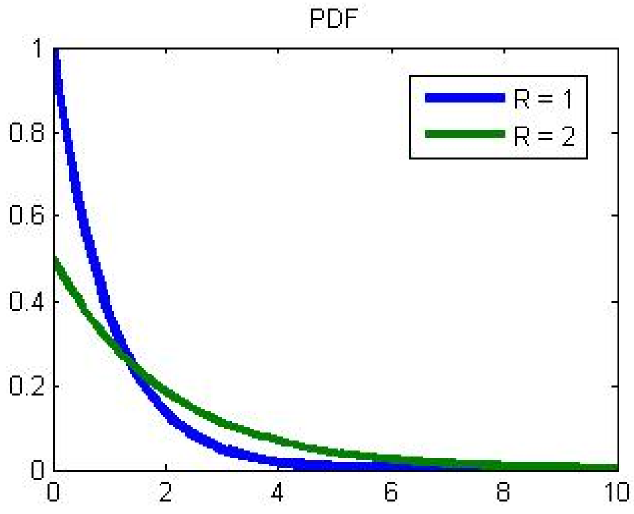
- $p_u \in [0,1]$: Local Protection Level.
- $p_a \in [0,1]$: Attack Level.
- $R \coloneqq r(p_u, p_a) = \log(\frac{p_a}{p_u} + 1)$: Risk Level.

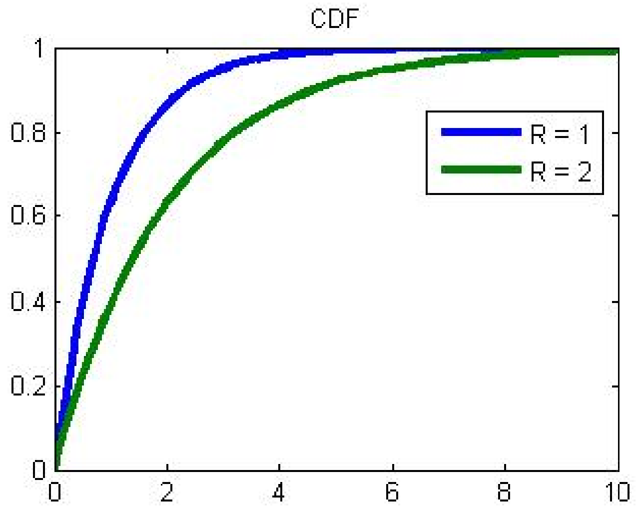


Case 1: 1 Node-1 User-1 Attacker-1 Insurer

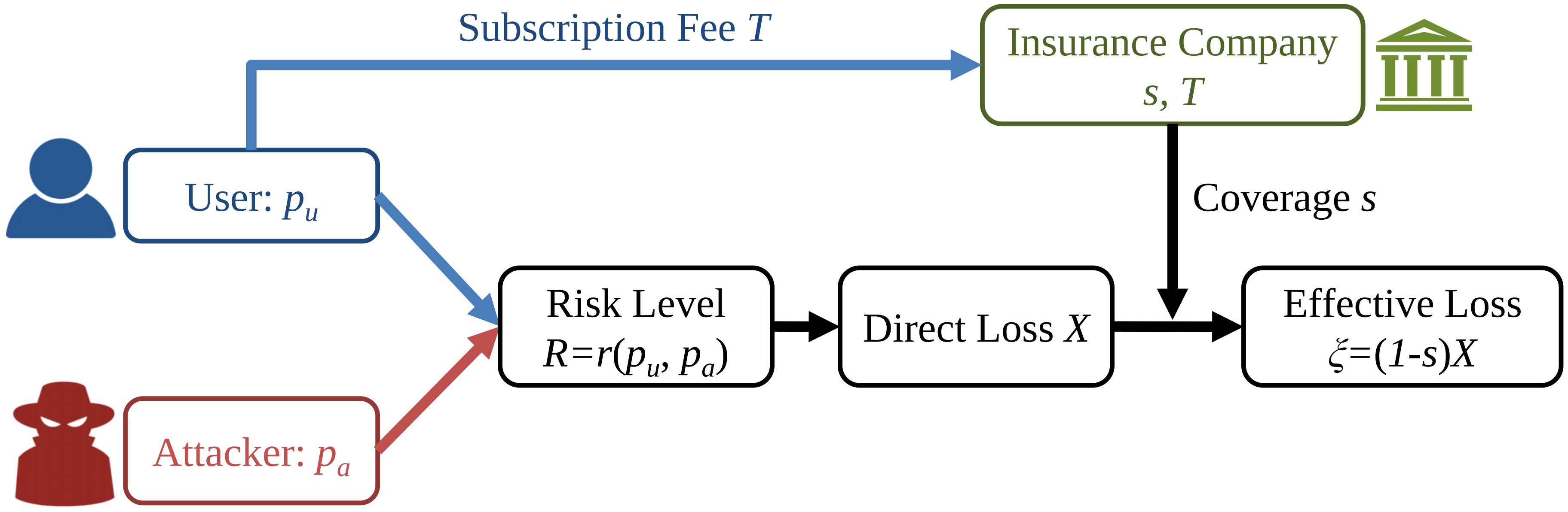


- $X \sim \exp(\frac{1}{R})$: Direct Loss.
- $f(x|R) = \frac{1}{R} e^{-\frac{1}{R}x}$.
- $\mathrm{E}[X] = R = \log(\frac{p_a}{p_u} + 1)$.





Case 1: 1 Node-1 User-1 Attacker-1 Insurer



- T: Subscription Fee.
- $s \in [0,1]$: Coverage Level.
- sX: Covered Loss.
- $\xi = (1 - s)X$: Effective Loss.
- $T - \mathrm{E}[sX]$: Insurer's Operating Profit.

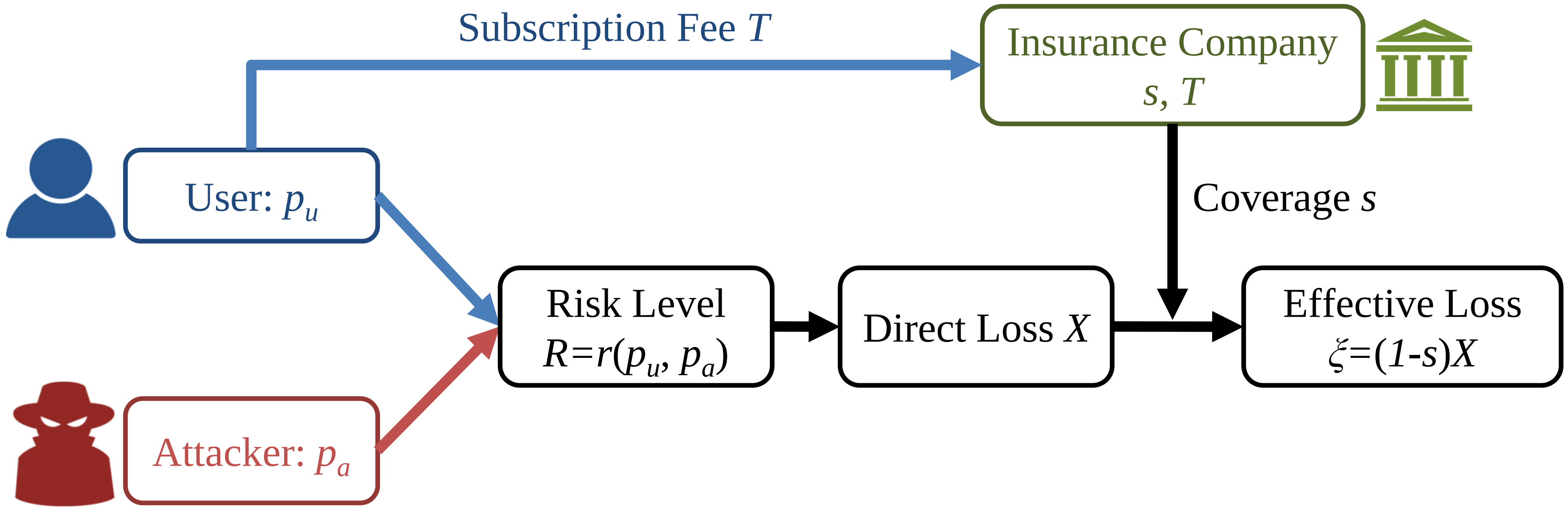
✓ Individual Rationality $(\mathrm{IR} - u)$:

$$\mathrm{E}[\xi] + T \leq \mathrm{E}[X].$$

✓ Individual Rationality $(\mathrm{IR} - i)$:

$$T - \mathrm{E}[sX] \geq 0.$$

Case 1: 1 Node-1 User-1 Attacker-1 Insurer

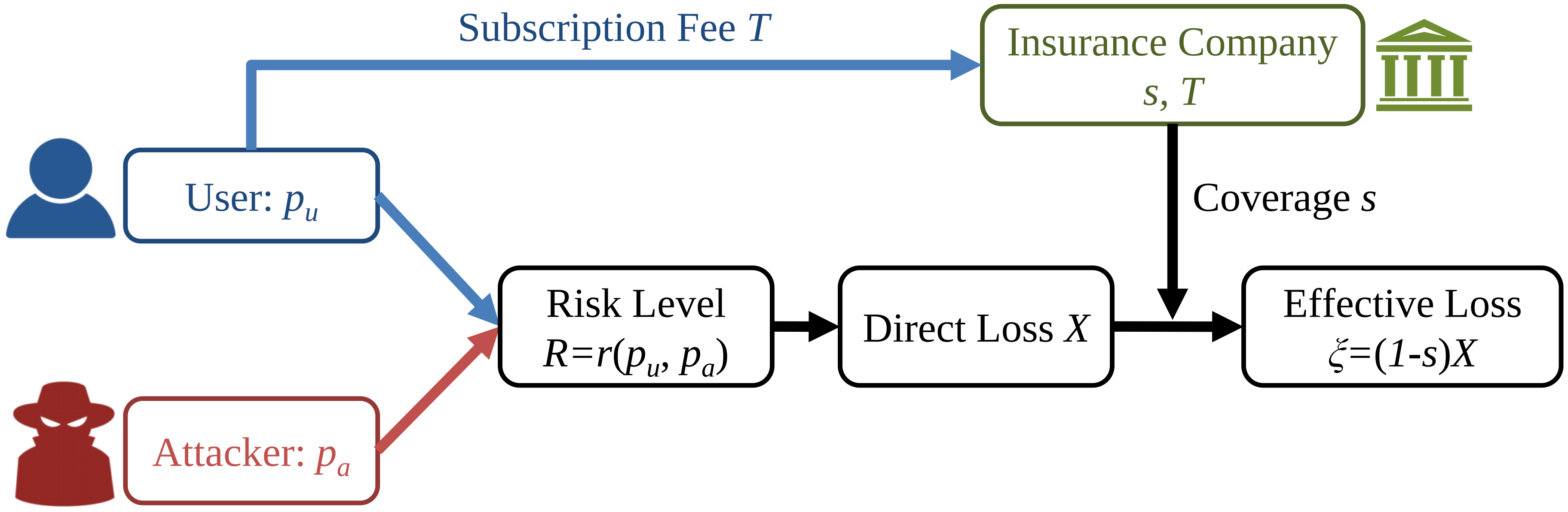


User and Attacker, Zero-sum Game, Complete Information:

- User: Reduce the average effective loss. Cost of Local Protections: c_u.
- Attacker: Enlarge the average effective loss. Cost of Cyber Attacks: c_a.
- Zero-sum Game:

$$\min_{p_u} \max_{p_a} \mathrm{E}[\xi] + c_u p_u - c_a p_a .$$

Case 1: 1 Node-1 User-1 Attacker-1 Insurer



User and Attacker, Zero-sum Game, Complete Information:

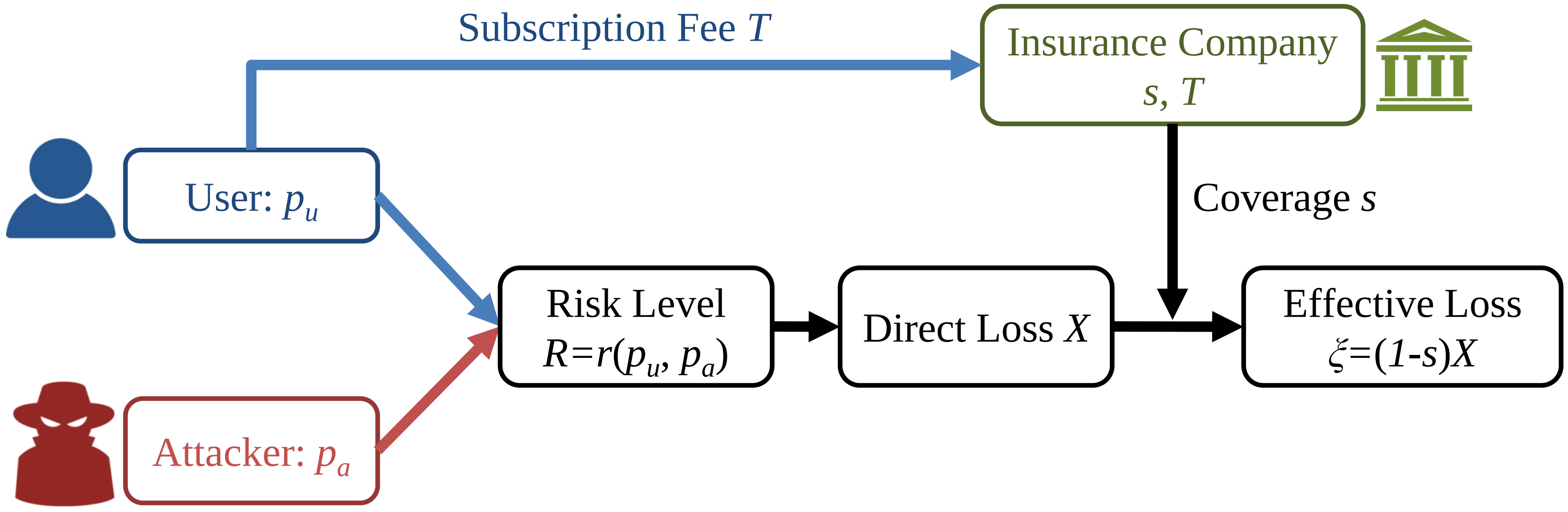
- Unique Saddle-Point Equilibrium (SPE):

$$p_u^* = \frac{(1-s)}{c_u+c_a}, p_a^* = \frac{c_u(1-s)}{c_a(c_u+c_a)}.$$

- Peltzman Effect: $s \uparrow, p_u^* \downarrow$.
- Constant Cost Determined SPE Risk:

$$R^* = \log(\frac{p_a^*}{p_u^*} + 1) = \log(\frac{c_u}{c_a} + 1).$$

Case 1: 1 Node-1 User-1 Attacker-1 Insurer



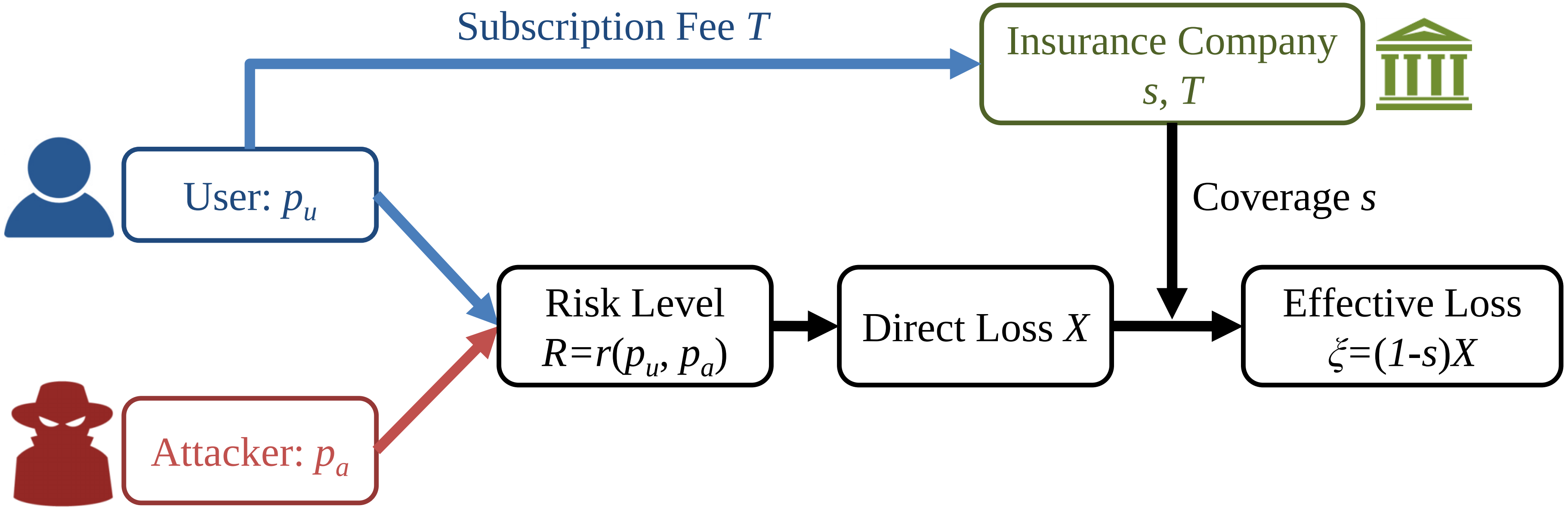
User and Insurer, Principal–agent Problem, Incomplete Information:

- Insurer: Make a profit and reduce the average effective loss of the user.
- c_i: Tradeoff between a larger profit of the insurer and a safer user.
- Insurer:

$$\max_{s,T}(T - \mathrm{E}[sX]) - (c_i\mathrm{E}[\xi])$$

$$\text{s.t.}\quad \begin{aligned} &\mathrm{E}[\xi] + T \leq \mathrm{E}[X]; \quad (\mathrm{IR}-u) \\ &T - \mathrm{E}[sX] \geq 0. \quad\ \ (\mathrm{IR}-i) \end{aligned}$$

Case 1: 1 Node-1 User-1 Attacker-1 Insurer



User and Insurer, Principal–agent Problem, Incomplete Information:

- Linear Insurance Policy Principle:

$$T = sR^*.$$

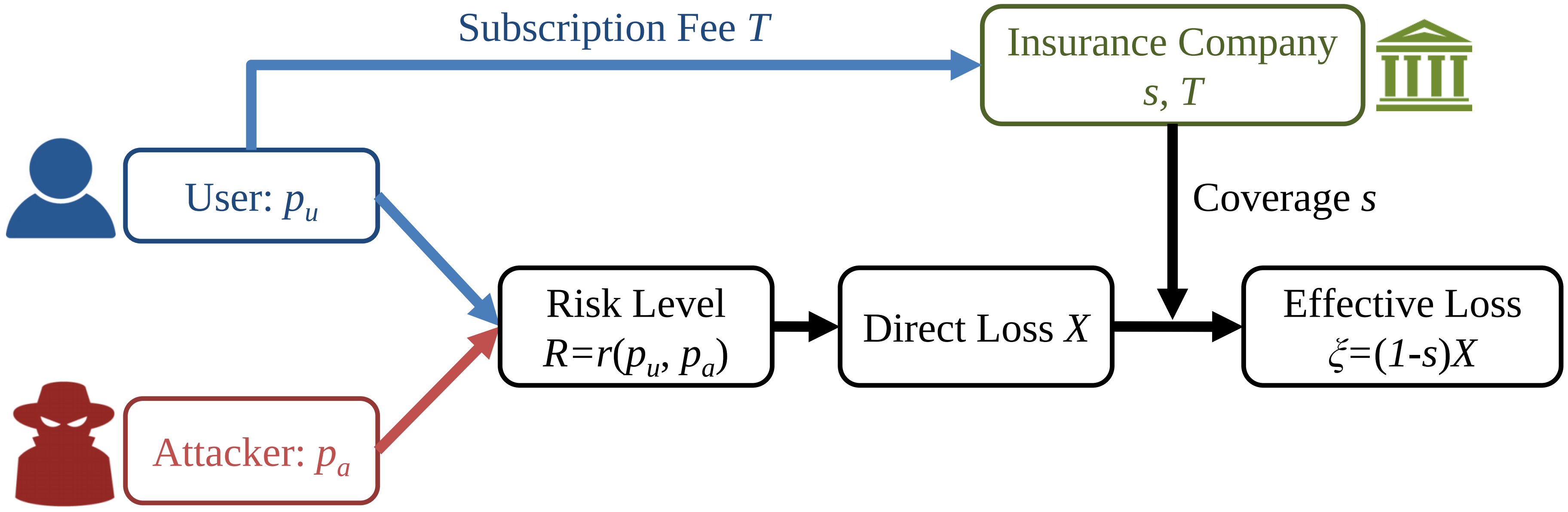
- Zero-operating Profit Principle:

$$T - sR^* = 0.$$

- Optimal Insurance Policy:

$$s^* = 1, T^* = R^*.$$

Case 1: 1 Node-1 User-1 Attacker-1 Insurer



User and Attacker, Zero-sum Game:

- Unique Saddle-Point Equilibrium (SPE):

$$p_u^* = \frac{(1-s)}{c_u+c_a}, p_a^* = \frac{c_u(1-s)}{c_a(c_u+c_a)}.$$

- Peltzman Effect: $s \uparrow, p_u^* \downarrow$.
- Constant Cost Determined SPE Risk:

$$R^* = \log(\frac{p_a^*}{p_u^*}+1) \ = \log(\frac{c_u}{c_a}+1).$$

User and Insurer, Principal–agent Problem:

- Linear Insurance Policy Principle:

$$T = sR^*.$$

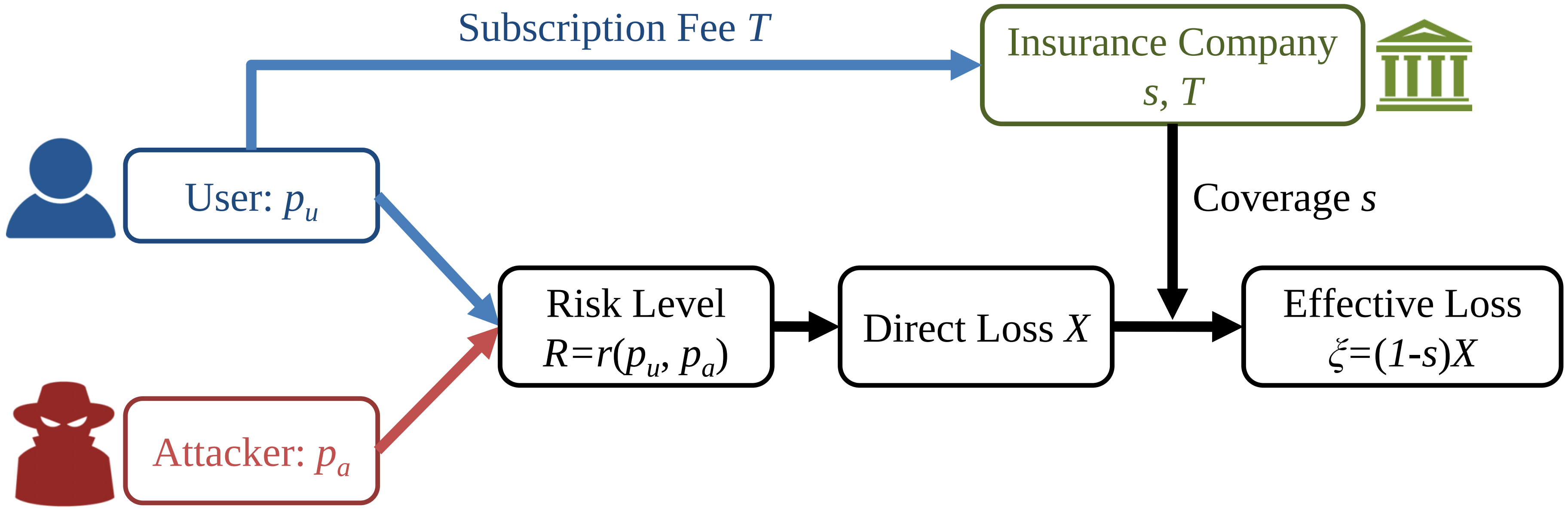
- Zero-operating Profit Principle:

$$T - sR^* = 0.$$

- Optimal Insurance Policy:

$$s^* = 1, T^* = R^*.$$

Case 1: 1 Node-1 User-1 Attacker-1 Insurer



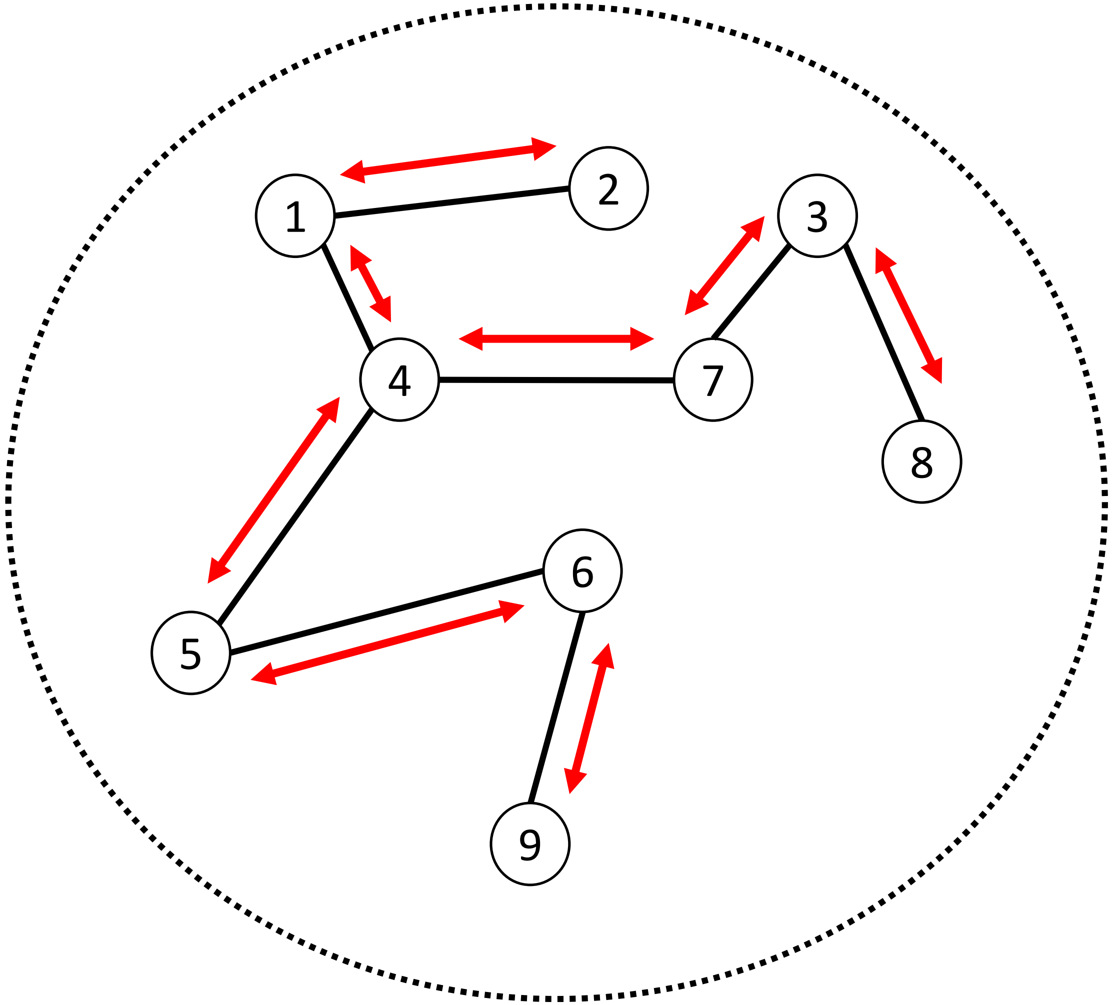
User, Attacker, and Insurer, Bi-level Game:

- Bi-level Game Nash Equilibrium:

$$s^* = 1, T^* = R^* = \log(\frac{c_u}{c_a} + 1)\,, p_u^* = 0, p_a^* = 0.$$

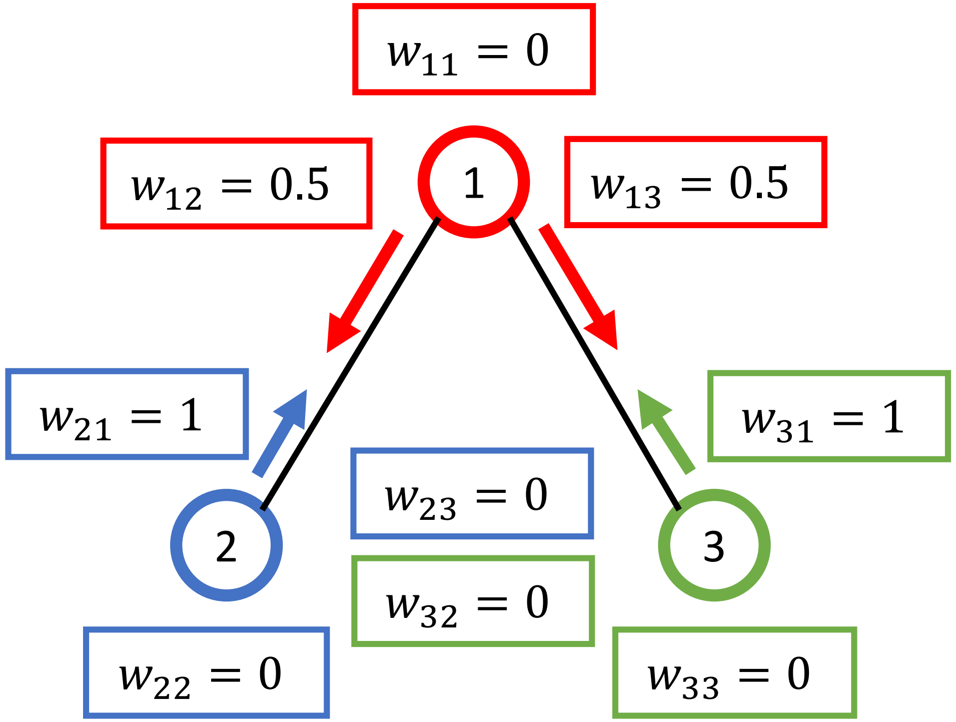
- Insurer: Full Coverage.
- User and Attacker: No actions.

Case 2(a),2(b),3: Network Effects



- Network: N Nodes, $n = 1, \dots, N$.
- Local Protection Levels: $p_{u,n}$.
- Attack Levels: $p_{a,n}$.
- Coverage Levels: s_n.
- Subscription Fees: T_n.
- Risk Levels: R_n.
- Direct Losses: X_n.
- Effective Losses: ξ_n.

Case 2(a),2(b),3: Network Effect



$$w_{11} + w_{12} + w_{13} = 1$$

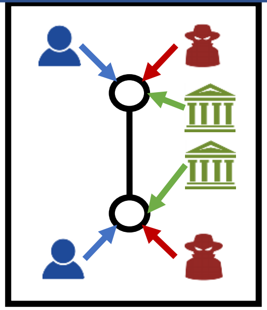
$$w_{21} + w_{22} + w_{23} = 1$$

$$w_{31} + w_{32} + w_{33} = 1$$

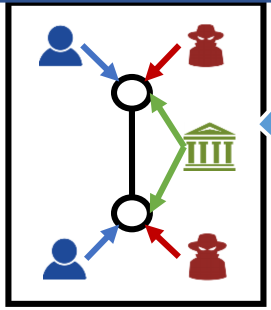
- w_{mn} : Probability that an attack on node m leads to an attack on node n,
$$w_{mm} = 0, \sum_{n=1}^{N} w_{mn} = 1, \forall n = 1, \dots, N.$$
- Risk Levels:
$$R_n := r(p_{u,n}, p_{a,n}) + \eta \sum_{m=1}^{N} w_{mn} R_m \,.$$
- $\eta \in [0,1]$: Scalability parameter of the network effect.
- $\mathbf{R} = \mathbf{r} + \eta \mathbf{W}^T \mathbf{R} \Longrightarrow \mathbf{R} = (\mathbf{I} - \eta \mathbf{W}^T)^{-1} \mathbf{r}.$
- $\mathbf{W}^* = (\mathbf{I} - \eta \mathbf{W}^T)^{-1}.$
- $R_n := \sum_{m=1}^{N} w_{nm}^* r(p_{u,m}, p_{a,m}).$
- $w_{nm}^* > 0, w_{nn}^* > 1, \forall n, m.$

Case 2(a),2(b),3: Zero-sum Games

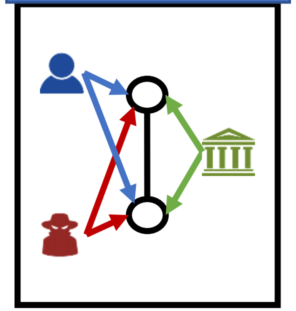
Case 2(a)



Case 2(b)



Case 3



$$\min_{p_{u,n}} \max_{p_{a,n}} K_n(\boldsymbol{p}_u, \boldsymbol{p}_a, s_n) = \mathrm{E}[\xi_n] + c_{u,n}p_{u,n} - c_{a,n}p_{a,n}$$

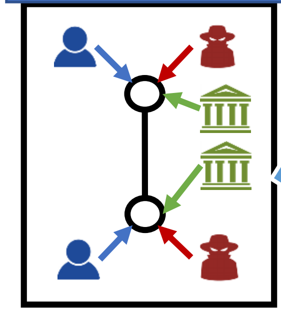
- $\mathrm{E}[\xi_n] = \mathrm{E}[(1-s_n)X_n] = (1-s_n)\mathrm{E}[X_n]$

$$= (1-s_n)R_n = (1-s_n)\sum_{m=1}^{N} w^*_{nm}\, r(p_{u,m}, p_{a,m}).$$

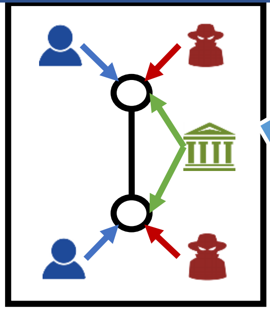
$$\min_{\boldsymbol{p}_u} \max_{\boldsymbol{p}_a} \sum_{n=1}^{N} K_n(\boldsymbol{p}_u, \boldsymbol{p}_a, s_n) = \sum_{n=1}^{N} \left(\mathrm{E}[\xi_n] + c_{u,n}p_{u,n} - c_{a,n}p_{a,n}\right)$$

Case 2(a),2(b),3: Zero-sum Games

Case 2(a)



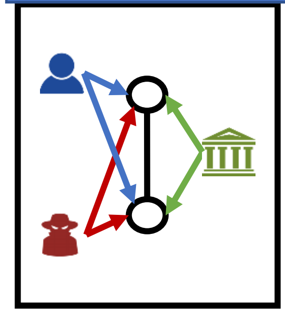
Case 2(b)



$$p^*_{u,n} = \frac{(1-s_n)w^*_{nn}}{c_{u,n}+c_{a,n}}$$

$$p^*_{a,n} = \frac{c_{u,n}(1-s_n)w^*_{nn}}{c_{a,n}(c_{u,n}+c_{a,n})}$$

Case 3



$$p^*_{u,n} = \frac{\sum_{m=1}^{N}(1-s_m)w^*_{mn}}{c_{u,n}+c_{a,n}}$$

$$p^*_{a,n} = \frac{c_{u,n}\sum_{m=1}^{N}(1-s_m)w^*_{mn}}{c_{a,n}(c_{u,n}+c_{a,n})}$$

Similarities:

- Unique Saddle-Point Equilibrium.
- Peltzman Effect.
- Constant Cost Determined SPE Risks:

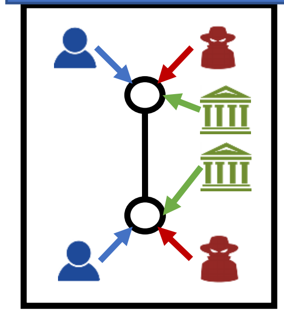
$$R^*_n = \sum_{m=1}^{N} w^*_{nm}\log(\frac{c_{u,m}}{c_{a,m}}+1)\,.$$

Differences:

- Actions: Case 3 > Case 2> Case 1.
- Actions: Case 3 depends on other nodes.
- SPE Risks: Case 2,3 > Case 1.

Case 2(a),2(b),3: Principal-Agent Problems

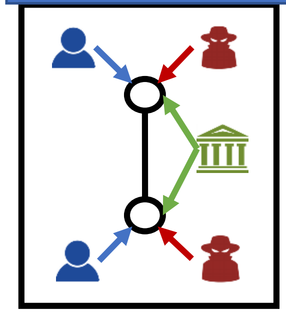
Case 2(a)



$$\max_{s_n,T_n}(T_n - \mathrm{E}[s_n X_n]) - (c_{i,n}\mathrm{E}[\xi_n])$$
$$\mathrm{s.t.}\quad (\mathrm{IR}-u,n),(\mathrm{IR}-i,n).$$

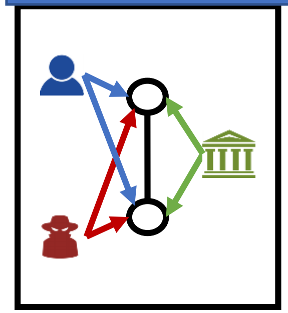
- Individual Rationality $(\mathrm{IR}-u,n)$:
  $$\mathrm{E}[\xi_n] + T_n \le \mathrm{E}[X_n].$$
- Individual Rationality $(\mathrm{IR}-i,n)$:
  $$T_n - \mathrm{E}[s_n X_n] \ge 0.$$

Case 2(b)



$$\max_{\boldsymbol{s},\boldsymbol{T}} \sum_{n=1}^{N}\big((T_n - \mathrm{E}[s_n X_n]) - (c_{i,n}\mathrm{E}[\xi_n])\big)$$
$$\mathrm{s.t.}\quad (\mathrm{IR}-u,n),(\mathrm{IR}-i,n), \forall n = 1,\dots,N.$$

Case 3

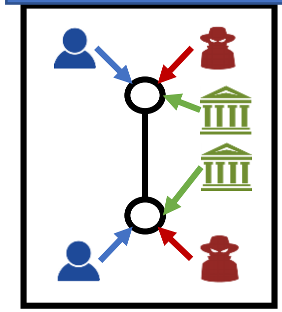


$$\max_{\boldsymbol{s},T} \sum_{n=1}^{N}\big((T - \mathrm{E}[s_n X_n]) - (c_{i,n}\mathrm{E}[\xi_n])\big)$$
$$\mathrm{s.t.}\quad (\mathrm{IR}-u),(\mathrm{IR}-i).$$

- Individual Rationality $(\mathrm{IR}-u)$:
  $$\sum_{n=1}^{N}\mathrm{E}[\xi_n] + T \le \sum_{n=1}^{N}\mathrm{E}[X_n].$$
- Individual Rationality $(\mathrm{IR}-i)$:
  $$T - \sum_{n=1}^{N}\mathrm{E}[s_n X_n] \ge 0.$$

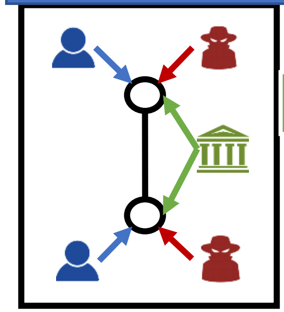
Case 2(a),2(b),3: Principal-Agent Problems

Case 2(a)



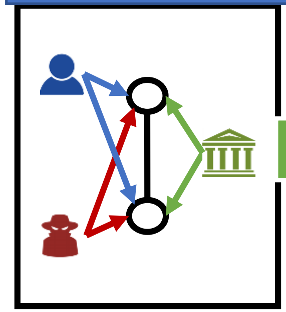
1. Linear Insurance Policy: $T_n = s_n R_n^*$.
2. Optimal Insurance Policy: $s_n^* = 1, T_n^* = R_n^*$.

Case 2(b)



1. Linear Insurance Policy: $T_n = s_n R_n^*$.
2. Optimal Insurance Policy: $s_n^* = 1, T_n^* = R_n^*$.

Case 3



1. Linear Insurance Policy:

$$T = \sum_{n=1}^{N} s_n R_n^* .$$

2. Optimal Insurance Policy:

$$s_n^* = 1, T^* = \sum_{n=1}^{N} s_n R_n^* .$$

Similarities:

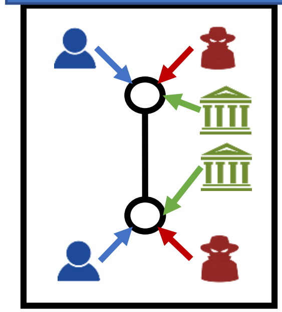
- Linear Insurance Policy Principle.
- Zero-operating Profit Principle.
- Full Coverage.

Differences:

- Subscription Fee: Case 2,3 > Case 1.

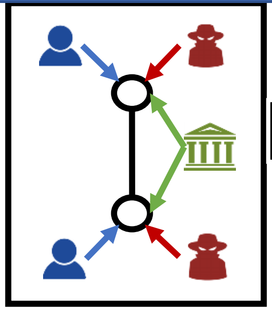
Case 2(a),2(b),3: Bi-level Games

Case 2(a)



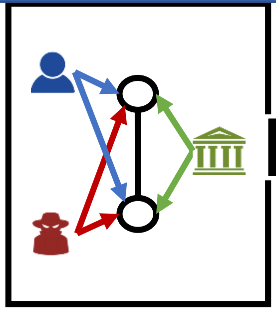
$$s_n^* = 1, T_n^* = R_n^*;$$
$$p_{u,n}^* = 0, p_{a,n}^* = 0.$$

Case 2(b)



$$s_n^* = 1, T_n^* = R_n^*, \forall n;$$
$$p_{u,n}^* = 0, p_{a,n}^* = 0.$$

Case 3



$$s_n^* = 1, \forall n, T^* = \sum_{n=1}^{N} R_n^*;$$
$$p_{u,n}^* = 0, p_{a,n}^* = 0, \forall n.$$

Similarities:
- Insurers: Full Coverage.
- Users and Attackers: No Actions.

Differences:
- Subscription Fee: Case 2,3 > Case 1.

Contributions:

- We have proposed a bi-level game-theoretic framework that incorporates a zero-sum security game nested with a principal-agent model.
- We have studied four distinct scenarios including single node case, centralized and decentralized network cases. For each scenario, the solution of the optimal insurance mechanism design problem is completely characterized.
- We have shown the Peltzman effect that the user tends to be risky when he subscribes the insurance.
- We have shown the linear insurance policy principle and the zero-operating profit principle of the insurer.

Future Directions:

- Dynamic setting;
- Data-driven decision-making;
- Complex networks.