Towards a Cooperative Defense Model Against Network Security Attacks

Harikrishna[1], Venkatanathan[1] and Pandu Rangan[2]

[1]College of Engineering Guindy, Anna University Chennai,Tamil Nadu, India

[2]Indian Institute of Technology, Madras, Tamil Nadu, India

Outline

Motivation

- People invest in security only if the loss due to a security attack is sufficiently high.
- Individuals who do not secure themselves become vulnerabilities for everyone else in a network.
- Users who desperately need security will contribute to the cost of protection of unprotected network users

Motivation

- People invest in security only if the loss due to a security attack is sufficiently high.
- Individuals who do not secure themselves become vulnerabilities for everyone else in a network.
- Users who desperately need security will contribute to the cost of protection of unprotected network users

Is cooperation possible to assure better security? How?

Outline

Related Work

Security Games

A game-theoretic model that captures the essentials of decision making to protect and self-insure resources within a network.

- First proposed by Varian (2002) and extended by Grossklags et al. (2008).
- Grossklags et al. consider two types of security investments:
  - Self-protection: e.g. firewalls & IDS.
  - Self-insurance: e.g. backup technologies.
- The model has also been extended with heterogeneous players and incomplete information.
- All existing models assume that the players are **non-cooperative**.

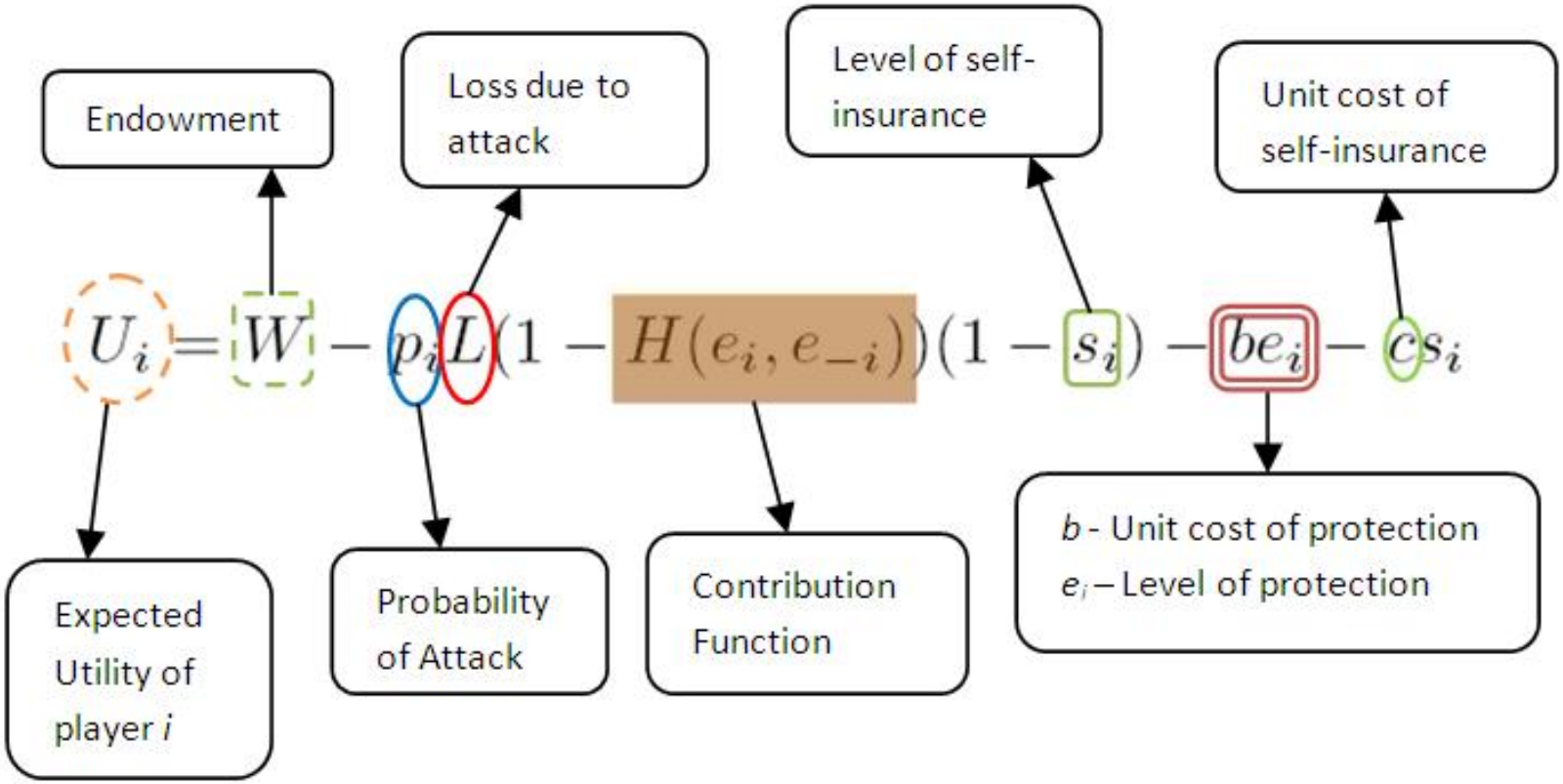
Outline

Our Contribution

- We introduce the notion of 'joint protection', where one or more users subsidize the protection efforts of other users.
- We also introduce heterogeneity in **player attitude** in the form of pessimism and optimism.
- Using Cooperative Game Theory, we model security games as **Partition Function Games (PFGs)**.

Outline

Grossklag's Utility Function



Contribution Functions

- The contribution function H characterizes the effect of a player's protection level, subject to the protection level of other players.
- **Weakest Link Game:** $\boxed{H(e_i, e_{-i}) = min(e_i, e_{-i})}$
  Example: Weak passwords in a network.
- **Total Effort Game:** $\boxed{H(e_i, e_{-i}) = \frac{1}{n}\sum_{k=1}^{n} e_k}$
  Example: In distributed file transfer services, an attacker's motive is to slow down the rate of file transfer.
- **Best Shot Game:** $\boxed{H(e_i, e_{-i}) = max(e_i, e_{-i})}$
  Example: To censor a piece of information, attacker has to ensure that no single copy of the information is available in the network.

Outline

Types of Defenders

Active Player:

- Have an incentive to protect themselves.
- Expected loss due to attack is L_a.
- Protection is cheaper for him when compared to the expected loss due to an attack and the insurance cost.

$$b = min(L_a, b, c)$$

Passive Player:

- Have no incentive to protect themselves and remain passive.
- Expected loss due to attack is L_p.
- Passivity is cheaper than self-protection and self-insurance.

$$L_p = min(L_p, b, c)$$

Assumption: Self-insurance is more expensive than self-protection ($c > b$).

Need For Cooperation

- Full protection is a social optimum, but is difficult to achieve when players are competitive.
- In the weakest-link and total effort games, **full protection is not possible even if a single player is passive**.
- In the best shot game, **full protection is possible only if one player protects, while all other free ride on him**.
- In cases where competition fails, can full protection be achieved through cooperation?

Cooperative Model

- The three canonical security games are modeled as coalitional games.
- We define cooperation as **the willingness of players to form a coalition and contribute to the cost of protection of the entire coalition.**
- In a coalition, active players contribute to the cost of protection of the passive players.
- A value is associated with each coalition, which is shared among the coalitional members.

Outline

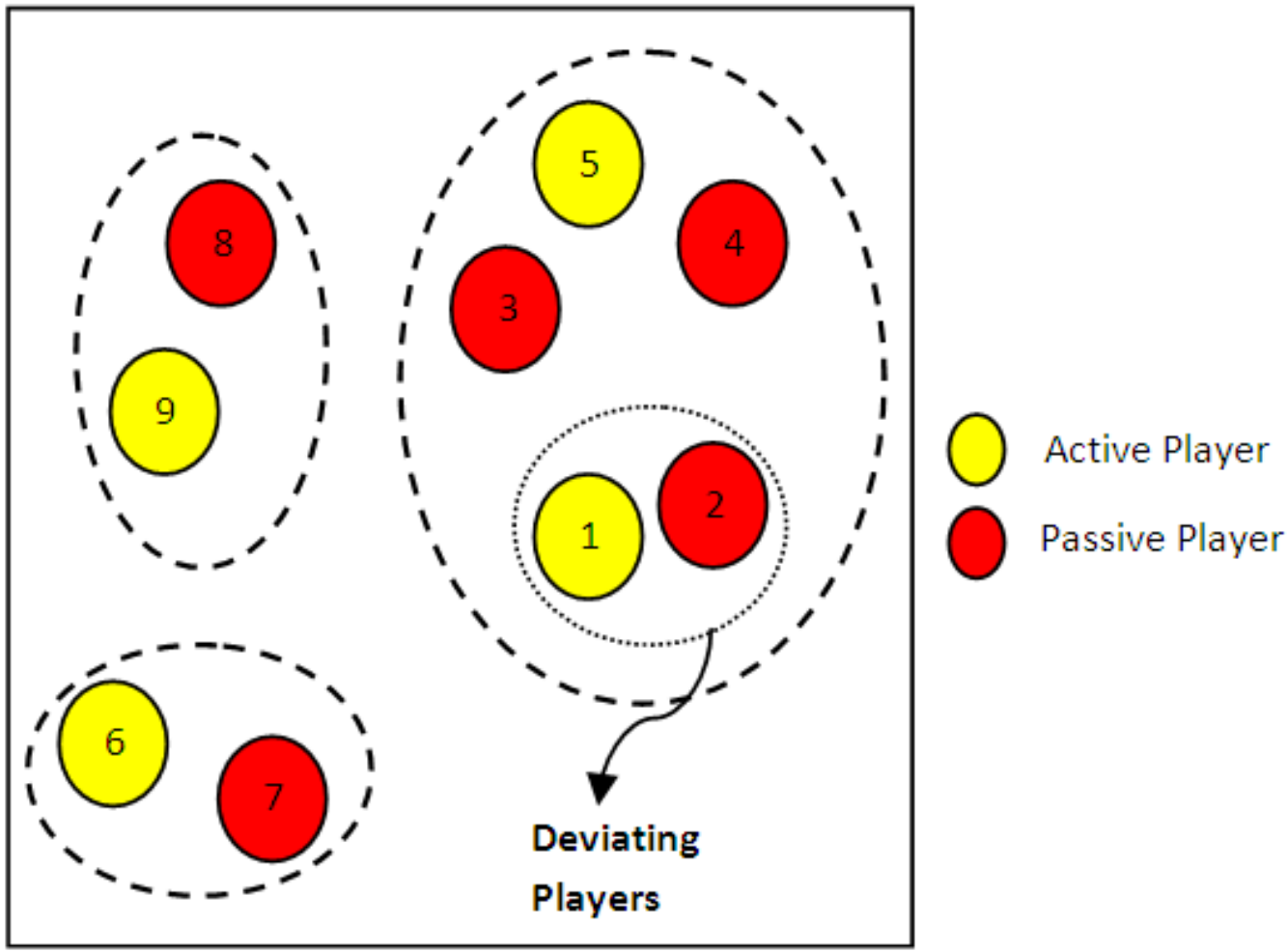
Partition Function Games (PFGs)

We utilize PFGs to design the cooperative model for the three canonical security games.

- Introduced by Thrall and Lucas (1963) to model coalition formation with externalities.
- Given a set of players N, any non-empty subset of players is a coalition.
- A partition $\mathcal{P}$ is a set of disjoint coalitions whose union is N.
- We denote the value assigned to a coalition P in partition $\mathcal{P}$ as $V(P, \mathcal{P})$.
- Each player is *allocated a part of his coalition's value* called payoff.

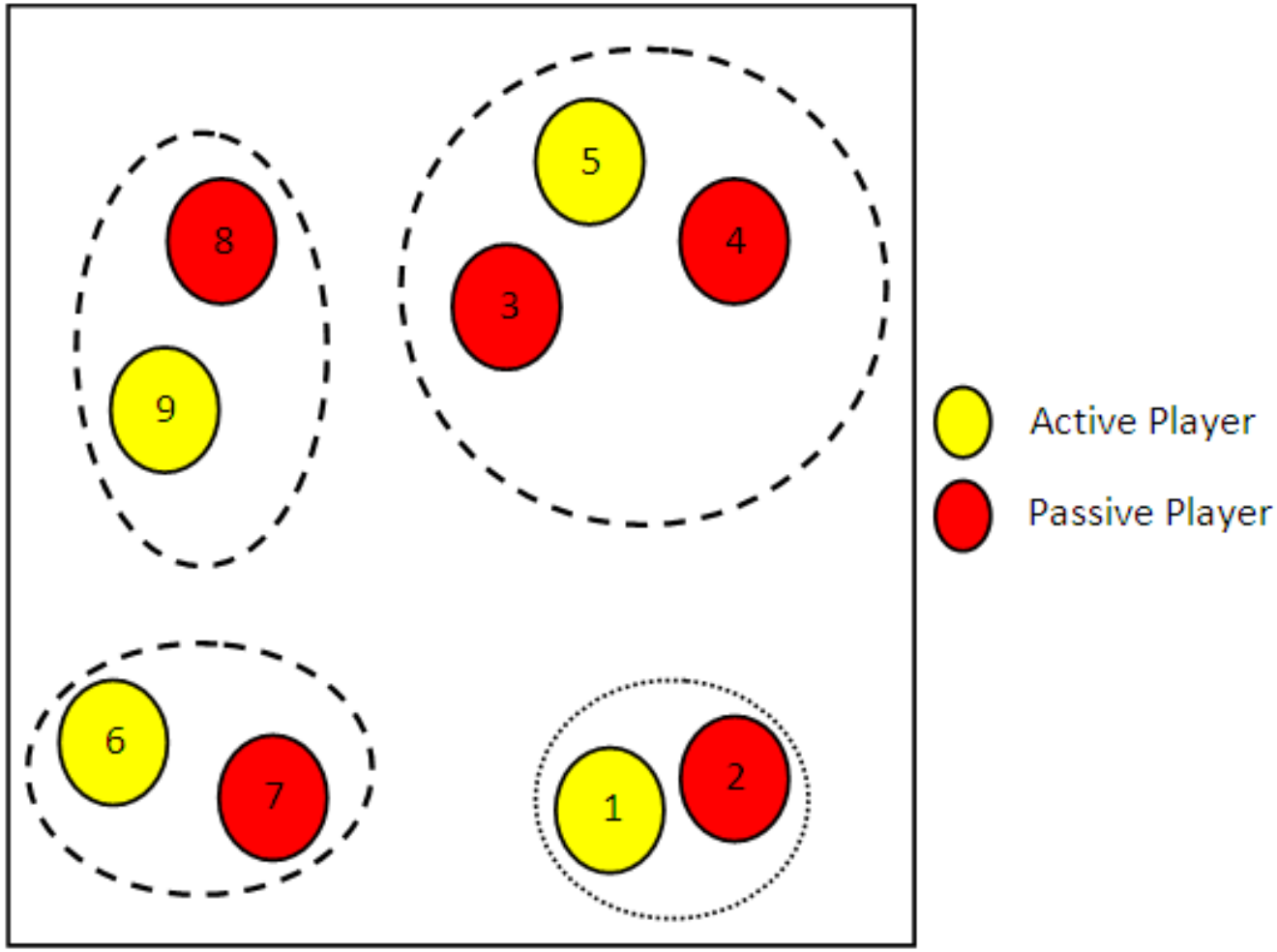
Deviation

- Given a partitioning of players, a set of players may choose to deviate from the current setup.



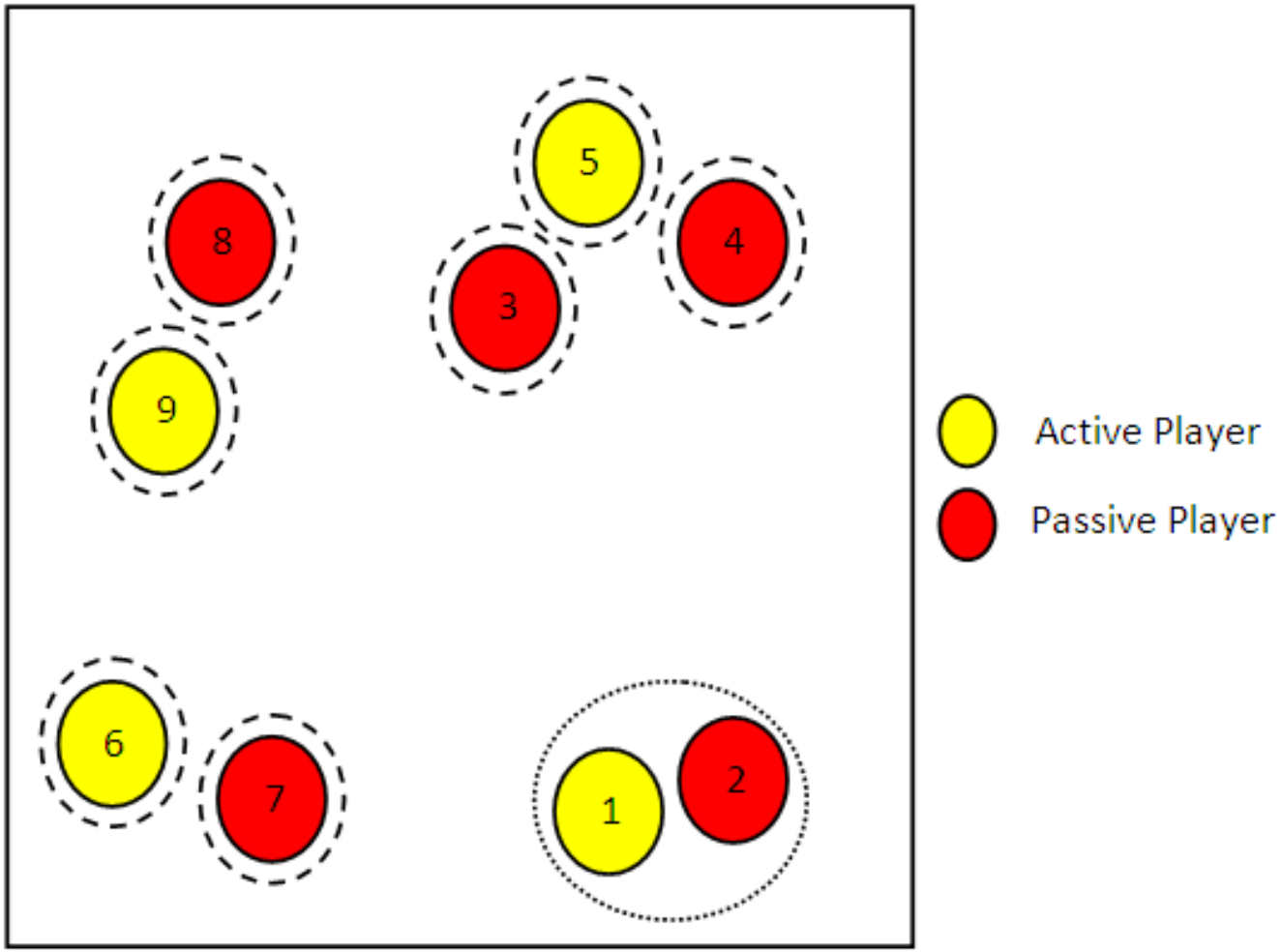
Optimism

- If the players are optimistic, they expect the best possible outcome after deviation.



Pessimism

- If the players are pessimistic, they expect the worst possible outcome after deviation.



Core

Core

The core is a set of partitioning of players along with their allocated payoffs, where no player has an incentive to deviate.

- The success of cooperation in a security game depends on the **non-emptiness of the core**.
- Two types of core.
  Optimistic Core: Assumes optimistic player attitude.
  Pessimistic Core: Assumes pessimistic player attitude.
- It can be shown that in a security game, a non-empty core would contain an outcome with the **grand coalition** of all players.

Outline

Notion of Surplus and Deficit

- Surplus is the maximum contribution of an active player towards the protection of passive players in the coalition.

$$surplus = E_{an} - E_{ac}$$

- E_{an}: Expenditure incurred by an **active player** when there is **no cooperation**
- E_{ac}: Expenditure incurred by an **active player** when he **cooperates**

- Deficit is the additional amount of money that a passive player requires if he needs to engage in full protection.

$$deficit = E_{pc} - E_{pn}$$

- E_{pc}: Expenditure incurred by a **passive player** when he **cooperates**
- E_{pn}: Expenditure incurred by a **passive player** when there is **no cooperation**

Weakest-link Game

- Consider a coalition P with l active players and k passive players. If every player outside P is protected,

$$V(P, \mathcal{P}) = l \times surplus - k \times deficit$$

- For a weakest-link game,

$$surplus = L_a - b = \alpha(say)$$

$$deficit = b - L_p = \beta(say)$$

- Then,

$$V(P, \mathcal{P}) = l\alpha - k\beta$$

Weakest-link Game: Pessimistic Core

Result: *The pessimistic core of a weakest-link security game with n_a active players and n_p passive players is non-empty if and only if*

$$\boxed{n_a\alpha - n_p\beta \geq 0}$$

Full protection is thus possible if:

- Players are **pessimistic**.
- The expected loss due to an attack for active players is **sufficiently high** that they prefer cooperation over non-cooperation.

Weakest-link Game: Optimistic Core

Result: *The optimistic core of a weakest-link security game with n_a active players and n_p passive players is non-empty if and only if*

1. $n_a\alpha - n_p\beta \geq 0$ and
2. **there exists no values** of $0 \leq l \leq n_a$ and $0 \leq k \leq n_p$ such that

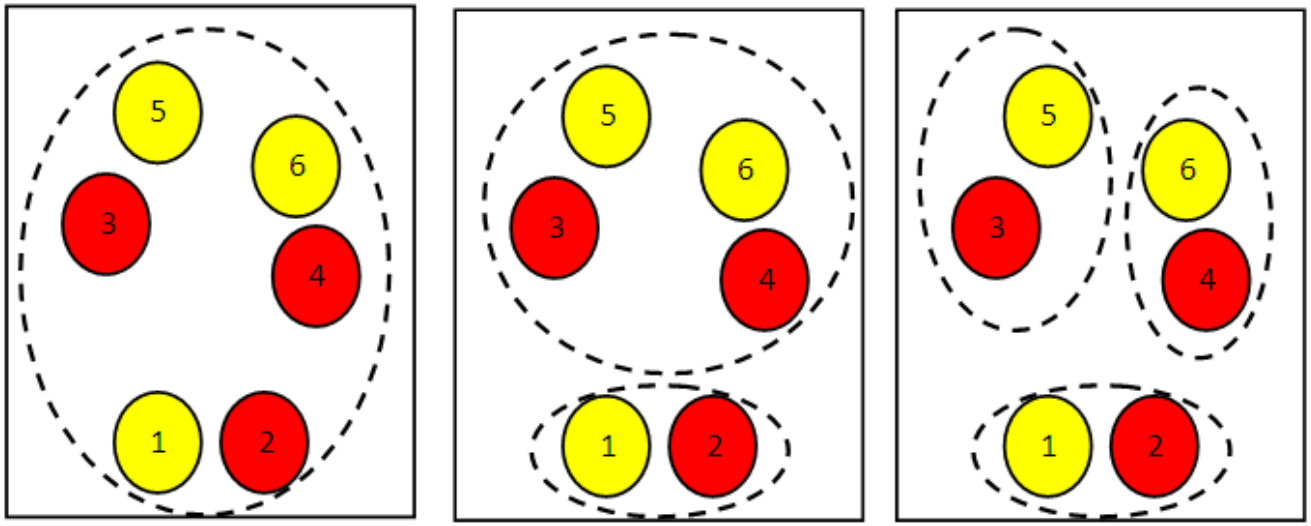
$$\boxed{\frac{k}{l} \neq \frac{n_p}{n_a}}$$

and $0 \leq l\alpha - k\beta \leq n_a\alpha - n_p\beta$.

Weakest-link Game: Optimistic Core (Continued)

When players are optimistic, full protection is possible if **one** of the following holds.

- The **grand coalition is the only formation**, where all passive players can be protected.
- There exists **multiple coalition structures** where all passive players are protected, but the **ratio between the number of passive and active players** in all the coalitions is equal to $\frac{n_p}{n_a}$.



Total Effort Game

- When there are n players, a player is assured of only $\frac{1}{n}^{th}$ **of his protection efforts**.
- A player self-protects only when his loss due to an attack is at least as high as n times the cost of protection.
- We assume that $L_a \geq nb$ for an active player and $L_p < b$ for a passive player.
- Here, we get

$$V(P, \mathcal{P}) = (k + r)(l\alpha' + k\beta') - kb,$$

where $\alpha' = \frac{L_a}{n}$ and $\beta' = \frac{L_p}{n}$

Core in a Total Effort Game

Results:

- *The* **pessimistic core** *of a total effort game with n_a active players and n_p passive players is non-empty.*
- *The* **optimistic core** *of a total effort game is non-empty if and only if there is exactly one active player in the game.*

Full protection is possible in a total effort game when **one** of the following holds.

- The players are optimistic, but there is **exactly one** active player in the network.
- The players are pessimistic, but there is **at least one** active player in the network.

Best Shot Game

- We define cooperation slightly different:

  The players take turns and protect themselves

  (or)

  A single player is self-protected throughout, while every one shares the cost of protection

- As long as a single active player is protected, passive players have no effect on the overall protection level and are not considered.
- Here,

$$V(P, \mathcal{P}) = IW - b$$

Core in a Best Shot Game

Results:

- *The* **pessimistic core** *of a best shot game with more than one active player is non-empty.*
- *The* **optimistic core** *of a best shot game with more than one active player is empty.*

Full protection is possible when **one** of the following holds true.

- There is **only one** active player in the network.
- There is **more than one** active player in the network, but all players are pessimistic.

Outline

Conclusions

- Full protection is difficult when the network contains one or more passive players. In such cases, the **players are better off cooperating** rather than competing.
- The success of joint protection efforts depends on the **attitude of the players** and the nature of the attack.
- In general, when the players are **optimistic** and the **network is large**, full protection becomes difficult to achieve.

References

1. Robert M. Thrall and William F. Lucas. n-person games in partition function form. *Research Logistics Quarterly*, 10(1):281–298, 1963.
2. Hal R. Varian. System reliability and free riding. In *the First Workshop on Economics of Information Security*, University of California, Berkeley, May 2002.
3. Jens Grossklags, Nicolas Christin, and John Chuang. Secure or insure? a game-theoretic analysis of information security games. In *Proceedings of the 17th International World Wide Web Conference (WWW '08)*, Beijing, China, April 2008, pages 209–218.

References (Contd.)

4 Jens Grossklags, Nicolas Christin, and John Chuang. Security and insurance management in networks with heterogeneous agents. In *Proceedings of the 9th ACM Conference on Electronic Commerce (EC '08)*, Chicago, Il, USA, July 2008, pages 160–169.

5 László A. Kóczy. The core of a partition function game. Technical report, KUL Centre for Economic Studies, Working Paper No. 25, November 2000.