



# Cheating Resistance of P2P Gaming Service Overlays

**Ikram M. Khan**, Kamill Panitzek, Max Lehn, Thorsten Strufe

5<sup>th</sup> Fachgespräch on Next Generation Service Delivery Platforms  
of the GI/ITG specialist group on Communications and  
Distributed Systems



Tuesday, Oct. 11, 2011 at DOCOMO-Labs,  
Munich, Germany

This work has been funded by the DFG research unit 733 QuaP2P.



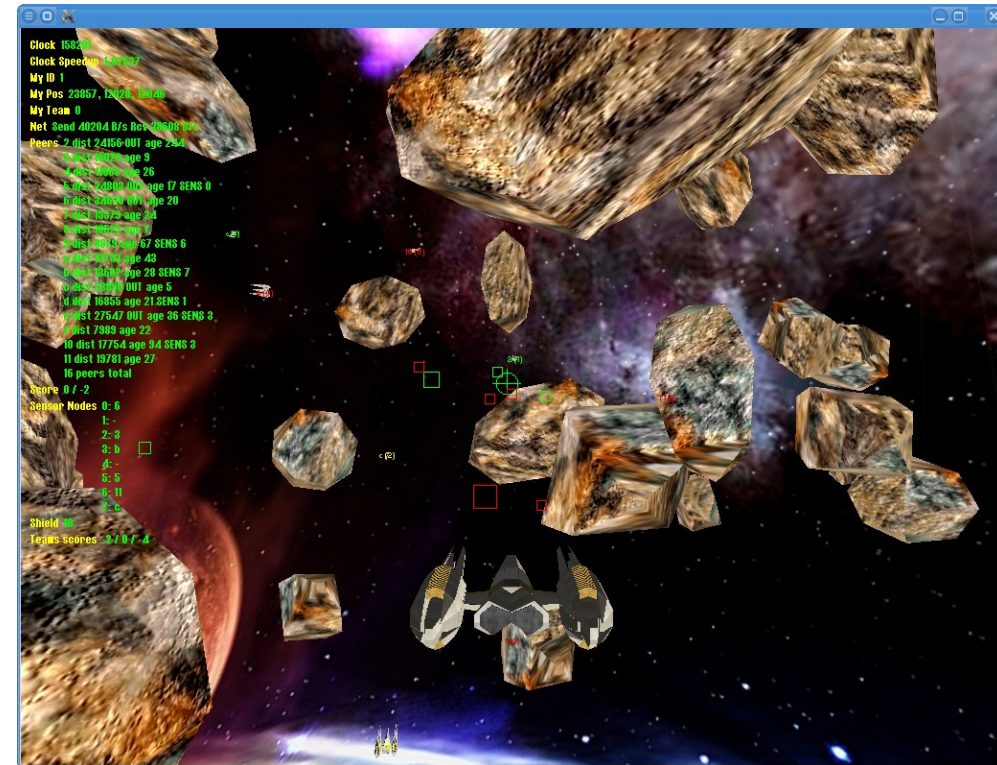
- Introduction
  - Motivation
  - Planet $\pi$ 4
  - Gaming service overlays
- Cheating resistance of gaming service overlays
  - Selected DoS attacks
  - Indirection scheme
- Security analysis and evaluation
- Summary and Outlook
- References





# Introduction - Planet $\pi$ 4

- Spaceship shooter
  - n players, m teams
- Asteroid field
  - Limits the effective game world dimensions
  - Full 3D or pseudo-2D (aligned to a plane)
- Points of Interest (POI)
  - Bases to be captured
  - Incentives: weapons, energy, ...
- Hotspots in player distribution





# Introduction – Gaming Service Overlays

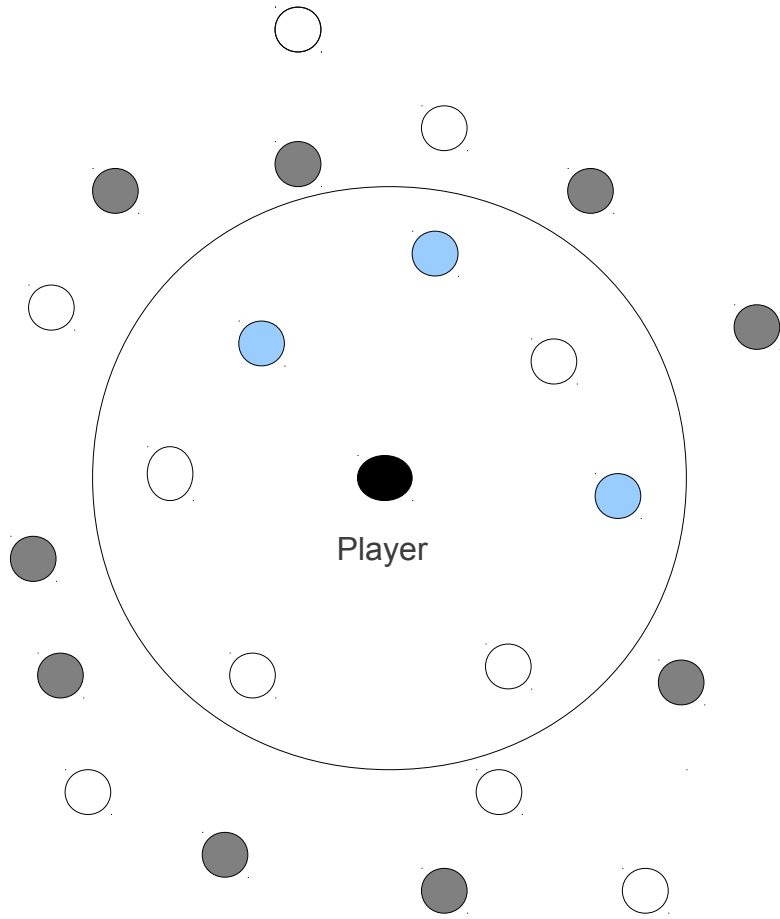


Fig: Virtual game world

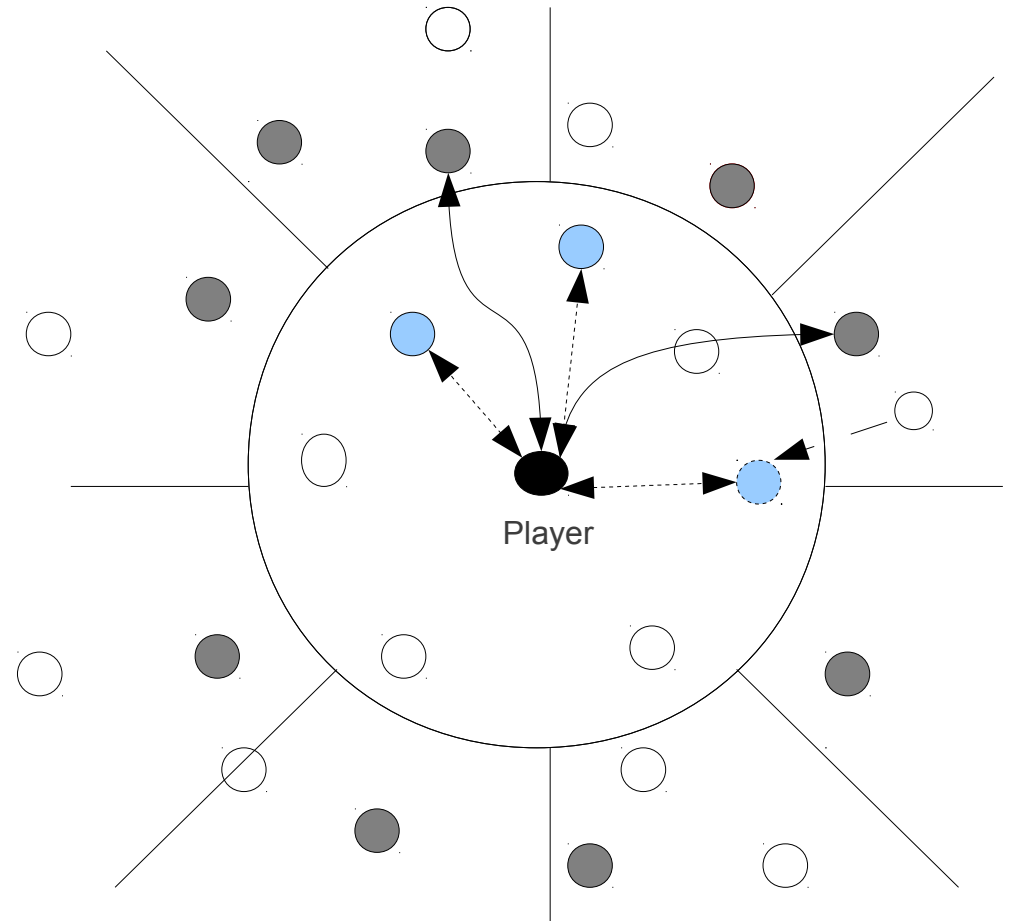


Fig: Candidate sensor nodes selections, pSense [1]

- Sensor nodes
- Newly arrived opponent
- Neighboring opponent
- Candidate sensor node
- Unknown nodes



# Cheating Resistance – Selected DoS Attacks

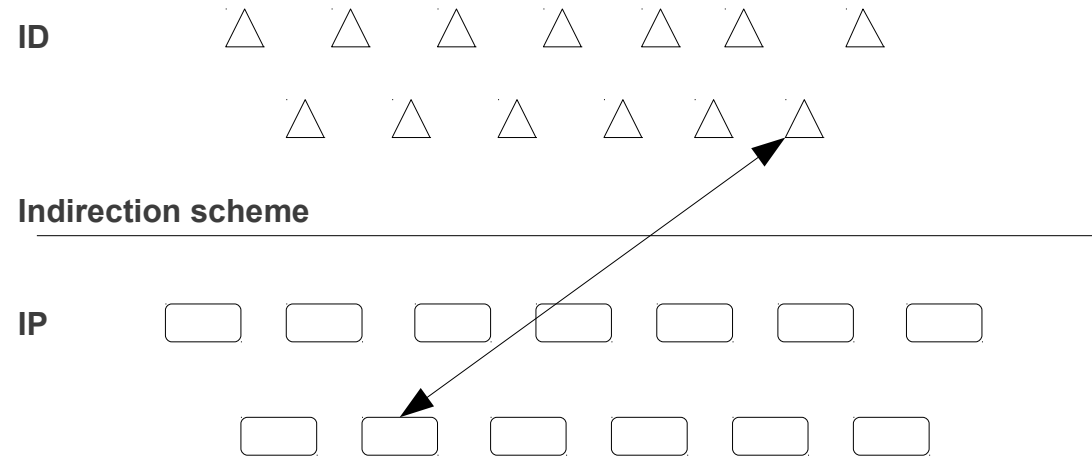
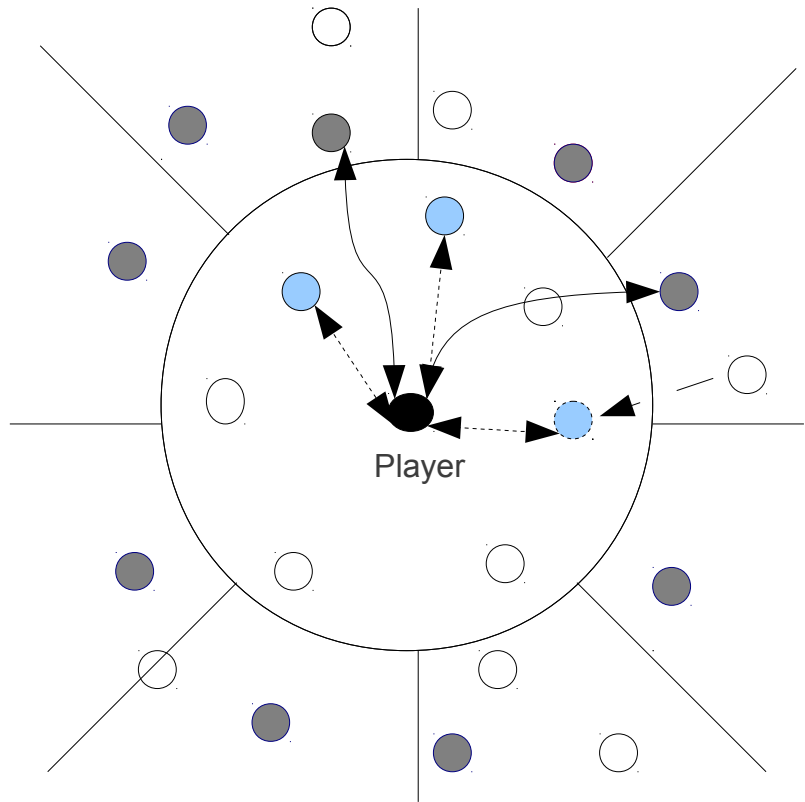
- Goal of an attacker
  - Map logical address (ID) with player's physical ID (IP)
  - Mapping leads to DoS attacks
- Assumed scenario
  - Open systems – adversary could see payload hence players' logical address (IDs)
- Key constraint(s)
  - Real-time requirements for first person shooter games e.g., delay  $\leq 300\text{ms}$  for real-time strategy games [2]
  - Un-linkability of sender/receiver IP - privacy



# Security Analysis and Evaluation

## Selected DoS attacks – gaming overlays

- Goal of an attacker
  - Map logical address (ID) with player's physical ID (IP)
  - Mapping leads to DoS attacks



- Neighboring opponent
- Candidate sensor node



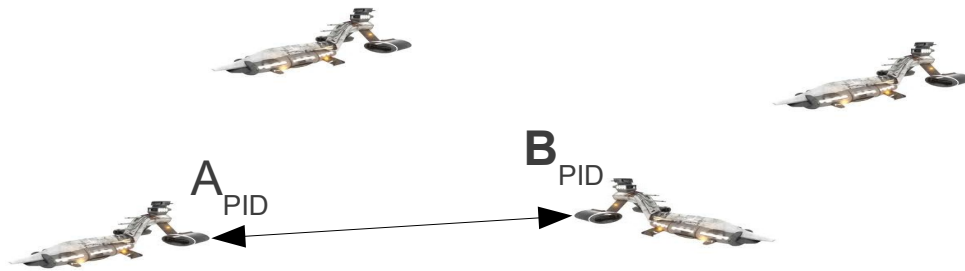
# Cheating Resistance - Indirection

- P. & H., *un-linkability* – items are no more and no less related than they are related concerning the a priori knowledge.
- => Black box to forward game information among players

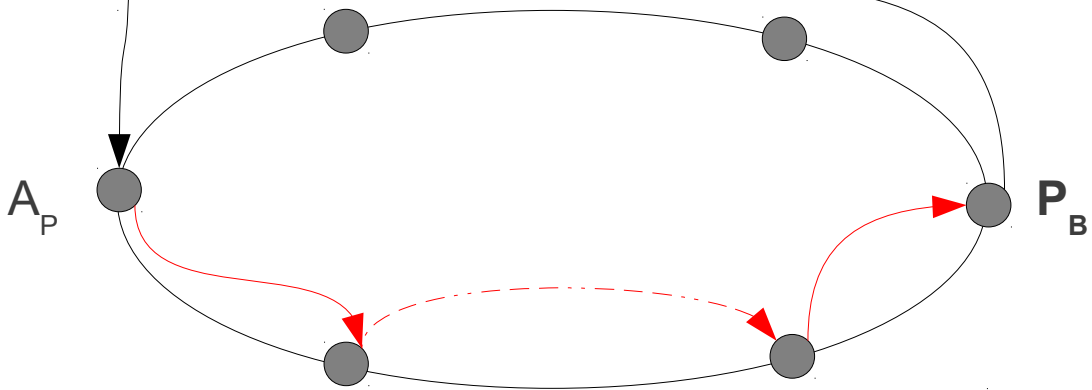


# Cheating Resistance - Indirection

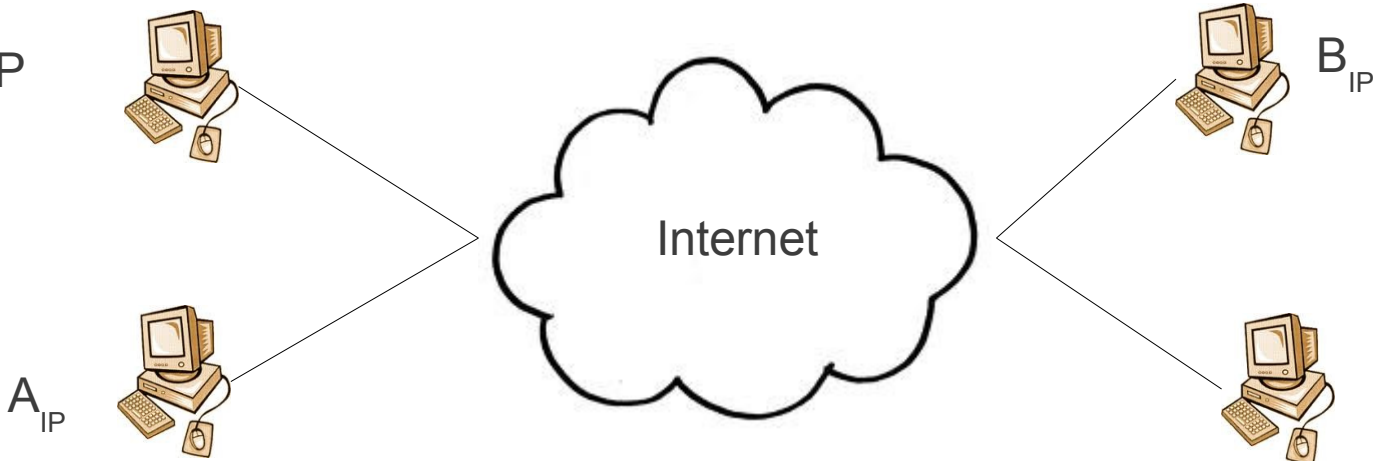
Game Service, PID



Indirection,  $P = H(IP)$



Underlay, IP





# Security Analysis and Evaluation

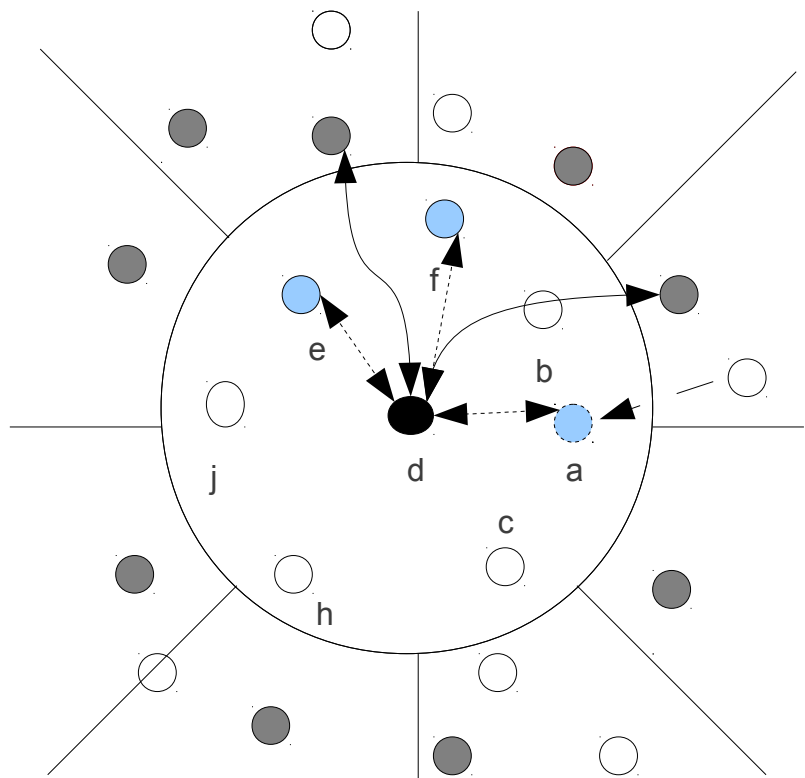
- How can anonymity be measured?
- Is there any anonymity metric which could be applied to indirection-scheme?
- How can we evaluate the effectiveness of attacks on the anonymity system?
- How can we quantify losses and gains in anonymity?
- How can anonymity metrics reflect the partial or statistic information often obtained by an adversary?



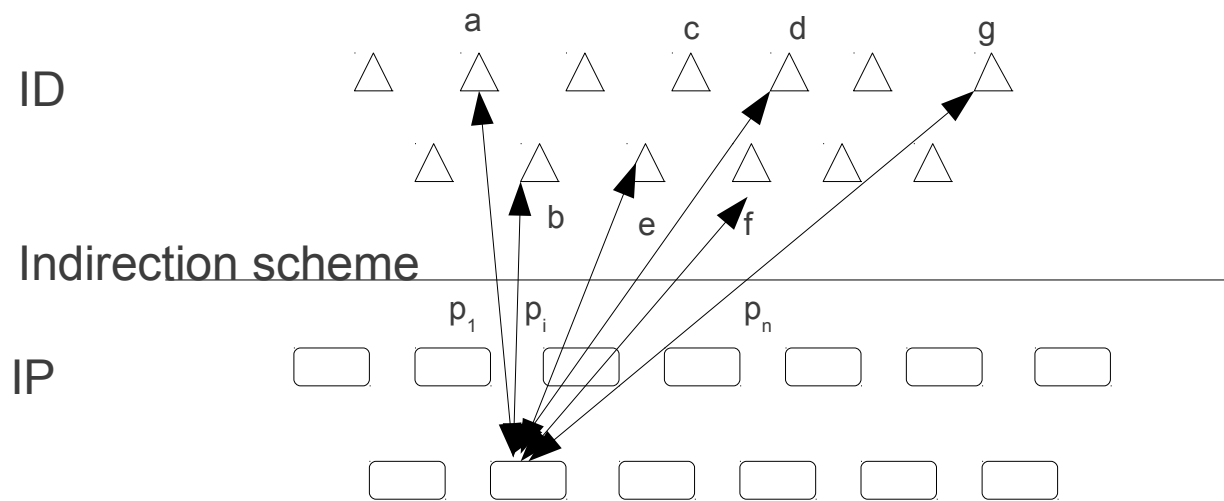
# Security Analysis and Evaluation

## Entropy-based Anonymity Metrics

- *S. & D., effective anonymity set* – the number of subjects (i.e., ID) linked to items of interest (i.e., IP) and the probabilities assigned to them
  - => The number of IDs linked to the IP
  - => Uniformity of the probability distribution



● Neighboring opponent ● Candidate sensor node for indirection



$$H(X) = - \sum_{i \in X} p_i * \log_2(p_i)$$



# Security Analysis and Evaluation

- S. & D., *effective anonymity set* – the number of subjects (i.e., ID) linked to items of interest (i.e., IP) and the probabilities assigned to them
  - => The number of IDs linked to the IP
  - => Uniformity of the probability distribution
- Diaz et al., *degree of anonymity* – is the ratio of effective anonymity set with maximum anonymity i.e.,  $H(X)/H_M$ 
  - => What degree of anonymity of the subjects can be achieved? Focuses on the performance of the scheme

How to assign probabilities to players?

How to measure the probabilities of indirection paths?



# Summary and Outlook

- Summary
  - Gaming service overlays
    - Un-availability due to DoS on players
  - Indirection scheme
    - Cheating resistance gaming service overlays
  - Security analysis and evaluation
- Outlook
  - Real-world implementation and integration to Planetπ4
  - Comprehensive security, performance, and QoE analysis



Questions?



# References

- [1] Arne Schmieg, Michael Stieler, Sebastian Jeckel, Patric Kabus, Bettina Kemme, and Alejandro Buchmann. pSense - Maintaining a Dynamic Localized Peer-to-Peer Structure for Position Based Multicast in Games. In IEEE International Conference on Peer-to-Peer Computing, 2008.
- [2] Mark Claypool, “The effect of latency on user performance in Real-Time Strategy games,” Elsevier North-Holland, Inc. New York, NY, USA, 2005.
- [3] P. & H. : Pfitzmann and Hansen, Anonymity, unobservability, and pseudonymity: a proposal for terminology.
- [4] S. & H. : Serjantov and Danezis, toward an information theoretic metric for anonymity.
- [5] Diaz et al., Reasoning about the anonymity provided by pool mixes that generate dummy traffic.
- [6] R. & R. : Reiter and Robin, Crowds: anonymity for web transactions.
- [7] B., P., & S. : Berthold, Pfitzmann, and Standtke, the disadvantages of free mix routes and how to overcome them.