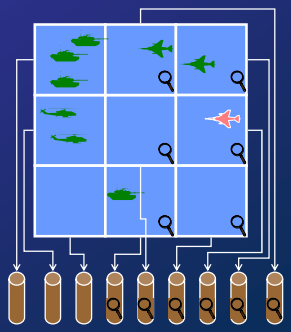
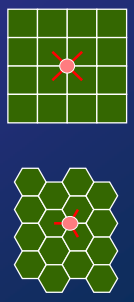
Group-per-Region Allocation

- Partition the world into regions and assign each region to a multicast group
- An entity transmits to groups corresponding to the region(s) that cover its location
- The entity subscribes to groups corresponding to interesting regions
- Entities have limited control over their nimbus but less control over their focus

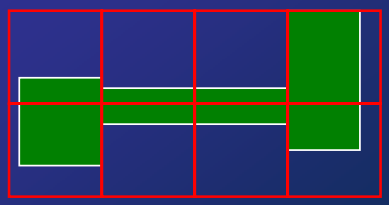


Region Bounds

- An entity has to change its target group(s) throughout its lifetime
  - track the bounds of the current region
  - learn the multicast address of a new region
  - boundaries and addresses assigned to the regions are often static
- In grid-based region assignment there are many points at which multiple grids meet
- Near these corners an entity has to subscribe to several groups

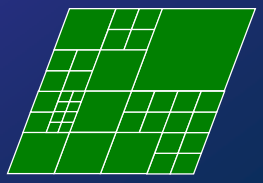


Environment vs. Regular Tessellation

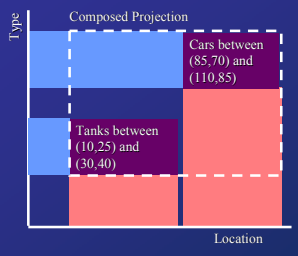


Hybrid Multicast Aggregation

- Balance between fine-grained data partitioning and multicast grouping
- Three-tiered interest management system:
  1. Group-per-region scheme segments data based on location
  2. Group-per-entity scheme allows receiver to select individual entities
  3. Area-of-interest filter subscriptions



Projections



- Projection aggregation server
  - collect data for a projection
  - transmit aggregated packets (projection aggregations)
- Projection composition
  - merge the interest specifications of the component projections

Compensating Resource Limitations: Recapitulation

- IPE: Resources = $M \times H \times B \times T \times P$
- Aspects:
  - consistency and responsiveness
  - scalability
- Protocol optimization
- Dead reckoning
- Local perception filters
- Synchronized simulation
- Area-of-interest filtering

§10 Cheating Prevention

- traditional cheating in computer games
  - cracking the copy protection
  - fiddling with the binaries: boosters, trainers, etc.
- here, the focus is on multiplayer online games
  - exploiting technical advantages
  - exploiting social advantages
- cheaters' motivations
  - vandalism and dominance
  - peer prestige
  - greed

The goals of cheating prevention

- protect the sensitive information
  - cracking passwords
  - pretending to be an administrator
- provide a fair playing field
  - tampering the network traffic
  - colluding with other players
- uphold a sense of justice inside the game world
  - abusing beginners
  - gangs



Network Security

- Military
  - private networks → no problem
- Business, industry, e-commerce,…
  - 'traditional' security problems
- Entertainment industry
  - multiplayer computer games, online games
  - specialized problems

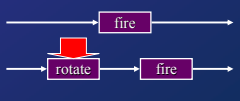


Taxonomy of Online Cheating 1 (4)

- Cheating by compromising passwords
  - dictionary attacks
- Cheating by social engineering
  - password scammers
- Cheating by denying service from peer players
  - denial-of-service (DoS) attack
  - clog the opponent's network connection


Taxonomy of Online Cheating 2 (4)

- Cheating by tampering with the network traffic
  - reflex augmentation
  - packet interception
  - look-ahead cheating
  - packet replay attack
- Cheating with authoritative clients
  - receivers accept commands blindly
    - requests instead of commands
    - checksums from the game state

Taxonomy of Online Cheating 3 (4)

- Cheating due to illicit information
  - access to replicated, hidden game data
  - compromised software or data
- Cheating related with internal misuse
  - privileges of system administrators
  - logging critical operations into CD-ROMs
- Cheating by exploiting a bug or design flaw
  - repair the observed defects with patches
  - limit the original functionality to avoid the defects
  - good software design in the first place!


Taxonomy of Online Cheating 4 (4)

- Cheating by collusion
  - two or more players play together without informing the other participants
  - one cheater participates as two or more players

- Cheating related to virtual assets
  - demand ⇒ supply ⇒ market ⇒ money flow ⇒ cheating

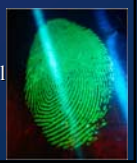
- Cheating by offending other players
  - acting against the 'spirit' of the game

Breaking the control protocol: Maladies & remedies

- *malady*: change data in the messages and observe effects
- *remedy*: checksums (MD5 algorithm)
- *malady*: reverse engineer the checksum algorithm
- *remedy*: encrypt the messages
- *malady*: attack with packet replay
- *remedy*: add state information (pseudo-random numbers)
- *malady*: analyse messages based on their sizes
- *remedy*: modify messages and add a variable amount of junk data to messages

MD5 algorithm

- message digest = a constant length 'fingerprint' of the message
- no one should be able to produce
  - two messages having the same message digest
  - the original message from a given message digest
- R. L. Rivest: MD5 algorithm
  - produces a 128-bit message digest from an arbitrary length message
- collision attack: different messages with the same fingerprint
- finding collisions is (now even technically!) possibl
  - what is the future of message digest algorithms?



Illicit information

- access to replicated, hidden game data
  - removing the fog of war
  - compromised graphics rendering drivers
- cheaters have more knowledge than they should have → passive cheating
- compromised software or data
- counter-measures in a networked environment
  - centralized: server maintains integrity among the clients
  - distributed: nodes check the validity of each other's commands to detect cheaters

Exploiting design defects

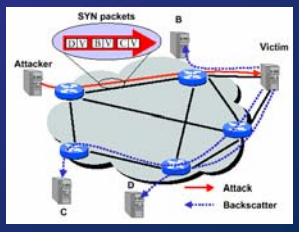
- what can we do to poor designs!
  - repair the observed defects with patches
  - limit the original functionality to avoid the defects
- client authority abuse
  - information from the clients is taken face-value regardless its reliability
- unrecognized (or unheeded) features of the network
  - operation when the latencies are high
  - coping with DoS and other attacks

Denial-of-Service (DoS) Attack

- Attack types:
  - logic attack: exploit flaws in the software
  - flooding attack: overwhelm the victim's resources by sending a large number of spurious requests
- Distributed DoS attack: attack simultaneously from multiple (possibly cracked) hosts
- IP spoofing: forge the source address of the outgoing packets
- Consequences:
  - wasted bandwidth, connection blockages
  - computational strain on the hosts

Analysing DoS Activity

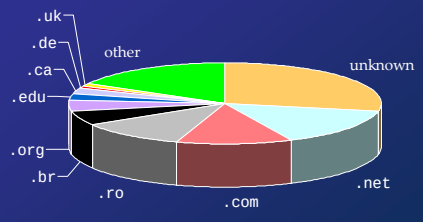
- Backscatter analysis
- Spoofing using random source address
- A host on the Internet receives unsolicited responses
- An attack of m packets, monitor n addresses
- Expectation of observing an attack: $E(X) = nm/2^{32}$



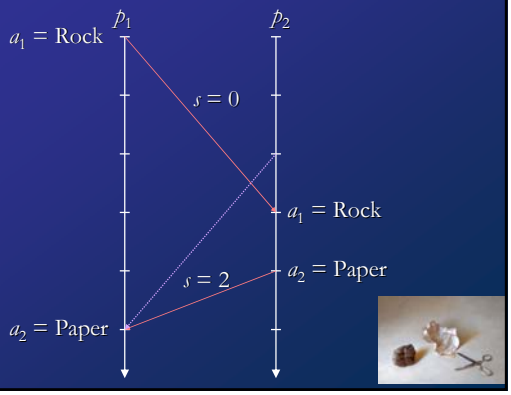
DoS: Selected Results

- Three week-long logging periods, February 2001
- >12,000 attacks, >5,000 distinct targets
- Significant number of attacks were directed against
  - home machines
  - users running Internet Relay Chat (IRC)
  - users with names that are sexually suggestive or incorporate themes of drug use
  - users supporting multiplayer games
- In addition to well-known Internet sites, a large range of small and medium sized businesses were targeted

DoS: Most Attacked Top-Level Domains



Look-ahead cheating



Two problems

- delaying one's decision
  - announce own action only after learning the opponent's decision
  - one-to-one and one-to-many
- inconsistent decisions
  - announce different actions for the same turn to different opponents
  - one-to-many