Quality of Service and Denial of Service

Stanislav Shalunov, Benjamin Teitelbaum

ACM SIGCOMM RIPQOS Workshop, Karlsruhe, Germany,
2003-08-27

QoS—Congestion Regulator

- Many factors might affect outcome of a network transaction
  - routing stability
  - physical connectivity
  - router stability
  - end-host capacity
  - network congestion

- QoS is only about controlling the effects of congestion
  - congestion is where most of the research has been
  - congestion is what we discuss in this talk

Terminology: Worst Case

- We'll often talk about the "worst case"

- Don't mean natural or man-made disasters, loss of physical connectivity, etc.

- QoS is about congestion

- "worst case" = worst possible offered load scenario

Worse Than Worst Case?

- Sometimes we'll mention, e.g., compromised routers
- These are not within the definition of worst case
- We don't think anything should protect against compromised routers
- It is still interesting to consider the damage a compromised router can do

Terminology: Elevated-Priority Services

- Two classes of QoS schemes:
  - Elevated-priority services
    - treatment better than that of best-effort service
    - some sort of service level assurance (relative or absolute)
    - e.g., based on expedited forwarding, assured forwarding
  - Non-elevated-priority services
    - treatment not better than that of best-effort service
    - no service level assurance
    - e.g., alternative best-effort, scavenger

Non-Elevated-Priority QoS

- Very promising area
- Could be very low cost
- Perhaps has better chances of deployment than elevated-priority QoS
- Need not be protected from DoS
- Not further discussed here

Terminology: DoS Prevention

- We do not expect non-elevated priority services to provide protection against DoS

- Elevated-priority services might (or might not) protect against DoS

- An elevated-priority service prevents DoS if communication between any pair of hosts using that service (possibly with reservation in place) cannot be affected by traffic load offered by other hosts

Elevated-Priority QoS Without DoS Prevention

- Costs
  - always present
  - operations, router cost, configuration, billing, etc.
  - current outside technical interface (IPv4 and BGP) changes to something more complex
  - costs are significant
- Benefits
  - Average case $\rightarrow$ same performance, chance of losses because of policers $\rightarrow$ small negative benefits
  - Worst case $\rightarrow$ perhaps marginally better chance of working $\rightarrow$ small positive benefits
  - Overall benefits are close to zero (perhaps positive, perhaps negative, but small absolute value)
- costs $\gg 0$, benefits $\approx 0 \rightarrow$ no deployment

Elevated-Priority QoS With DoS Prevention

- Costs
  - significant
  - similar to those without DoS prevention
- Benefits
  - Average case $\rightarrow$ again, slightly negative
  - Worst case $\rightarrow$ significant benefits
- costs $\gg 0$, benefits $\gg 0 \rightarrow$ possible deployment
  - With costs low enough, could be worth it
  - This is where elevated-priority QoS could bring value

Elevated QoS Problem Statement

- At times QoS seems like a solution in search of a problem
- To run pipes hot with adequate performance for all traffic?
  - Cheaper solutions exist: e.g., non-elevated QoS
- To deliver good performance to a class of traffic?
  - Cheaper solutions exist: e.g., overprovisioning
- To deliver better performance to demanding flows, but at a higher price?
  - Better solutions exist: e.g., congestion pricing
- To prevent DoS attacks?
  - This could bring value and remove the only real advantage circuit switching currently has over packet switching.

Statistical Network Provisioning

- Even without DoS, it is important to be ready for arbitrary traffic patterns
- Statistical provisioning can work well for voice
  - Any given user has very small impact on the traffic pattern
- Statistical provisioning does not work as well for data
  - Impact of individuals is much larger
  - Good sample sizes and traffic models needed for statistics
  - The relevant sample might consist of few individuals

DoS: A Fuzzy Concept

- Hypothetical question: Can we deploy other mechanisms that prevent DoS and not worry about DoS in other areas?
- If we don't want to be prepared for an *arbitrary* offered load pattern, we need to define DoS.
- Is automatic connection testing DoS?
- Are TCP throughput tests DoS?
- Are aggressive non-TCP throughput tests DoS?
- Is *intent* what defines DoS?
- There is no `intent` field in IP headers despite RFC3514!

No DoS Silver Bullet

- If we can't define DoS, we should not expect to be able to solve the DoS problem in isolation

- To prevent DoS technically, we must be prepared for an arbitrary offered traffic load

- Therefore, technical DoS prevention *is* a QoS problem

QoS Can Be One of the Mechanisms to Cope with DoS

- We do not claim that the best solution to DoS is technical

- We do not even claim that the problem of capacity saturation DoS has *any* acceptable solutions in packet networks

- We do believe, however, that exploring the technical solution space is important research and that this is the community with the expertise to do it

Thinking as an Adversary

- Goal: an elevated priority service that works under arbitrary traffic conditions
- Finding the worst condition is essential to understanding worst-case behavior
- Finding the worst condition is also what a malicious adversary would do
- *Need to think like an adversary*
- An architecture hardened against an adversary will also cover "natural" traffic variation

What Can a Compromised Host Do?

- What is the worst behavior of a single host?
- How could a host behave if taken over by a smart adversary?
- Would it send a continuous stream of a particular kind of reservations?
- Would it flood the net with some specially marked traffic?
- Would it impersonate routers?
- Would it impersonate other hosts?
- ...

What Can a Compromised Router Do?

- Strictly speaking, the question is outside the scope of the problem as stated

- However, it is still interesting and important to understand the damage a compromised router might inflict

- One generally assumes that routers are not compromised

- Yet it is important that one also knows what can happen if they are compromised

If Routers Are Compromised, is There Byzantine DoS Protection?

- Perhaps complete DoS protection in the face of compromised routers proves infeasible

- Could damage from a small number of unusually behaving neighbors be contained?

- Can one characterize and quantify the conditions under which reservations continue to work?

Is there DoS Protection if No Routers Compromised?

- Can a reservation continue to work under arbitrary traffic conditions?

- What are the sufficient conditions for this property?

- This would be the desired property

How Can Possibility of DoS be Controlled?

- Perhaps even this weaker property is not practical

- Are there parameters that a network provider can change to make it more difficult to conduct DoS attacks?

- What tools does a network engineer have to build networks resilient to DoS, even if they are not DoS-proof?

Security Compartments

- Can one contain the damage from unusually behaving hosts?
- Routers?
- Is it practical to split a network into logical administrative domains?
- How would this affect the percentage of traffic that can be dedicated to a higher-priority class?
- Operational complexity?

Operator Reaction to DoS

- Perhaps building DoS-resilient networks proves to be impractical
- How then should an operator respond to an ongoing DoS attack?
- Typical response today:
  - Black-hole traffic from specific sources
  - Apply filters that look for *ad hoc* traffic signatures
- Are there QoS-related mechanisms that would make the response better than the current response

Detection of DoS

- Perhaps providing better DoS remediation strategies proves to be impractical

- Could the QoS research community at least provide improved detection techniques?

- For example, is it possible to help with automated traffic signature generation?

Assume This Secure QoS Scheme Is Built

- *Assume* that one builds a network that prevents DoS
- *Assume* that the QoS techniques this network uses allow for easy damage compartmentalization
- *Assume* that they help with detecting DoS too (so they help best-effort traffic)
- *Assume* that primitives better than current filters are provided to respond to DoS
- Is the problem completely solved then?
- On a strictly technical level, yes.
- On an operational level that would affect deployment, no.

Service Verification for the Customer

- A customer who buys an elevated-priority service normally gets a service that's indistinguishable from best-effort

- Extra cost buys a guarantee rather than routine better service

- How is a guarantee verified?

As a Customer, Do I Get What I Paid For?

- Running under normal conditions does not verify a guarantee

- Unusual conditions (e.g., a DoS attack) might not happen frequently if at all

- Active measurement by sending in-profile traffic does not prove that the provider has actually engineered a guarantee

- Is recreating attack conditions the only way to technically verify a guarantee? (What ISP wants such customers?)

If Not Technical Verification, What Else?

- In other industries, when guarantees are provided, the customer does not need to know anything about their engineering

- Monetary reimbursement is generally accepted by customers

- Simple “your money back if it doesn’t work” is not enough

- Anything stronger hasn’t been accepted by providers

Service Verification for the Provider

- Suppose a provider want to engineer an honest guarantee
- How is the provider's situation different from the customer's when it comes to verifying it?
- A provider has access to router configuration and knows its own network
- Are inferences based on router configuration enough?

Router Configuration Inspection

- Mismatches between documented and actual behavior are common
- Complex emergent behavior is exhibited by routers
  - Behavior can depend on interactions between versions of router software and line card firmware
  - Features can require other features and fail silently in their absence
- A provider would never rely on configuration inspection to ensure that traffic can pass
- Actual traffic is exchanged after any changes in configuration (e.g., at least by running *ping*)

Active Measurement of QoS Guarantees

- To measure behavior under unusual conditions, unusual conditions must exist
- To verify protection against DoS, DoS needs to occur
- Creating test DoS attacks is not a realistic option

Conclusion

- When an elevated-priority QoS scheme is designed, we want (at least) this answered:
  - *What could happen if a determined attacker wanted to deny service to a particular host or pair of hosts?*

- Open question:
  - *If QoS is insurance against DoS, how, short of mounting test DoS attacks, does one verify a guarantee?*

Author Contact Information

Stanislav Shalunov ⟨shalunov@internet2.edu⟩

Benjamin Teitelbaum ⟨ben@internet2.edu⟩

Questions?