Survey of Network-Based Defense Mechanisms Countering the DoS of DDoS Problems

Accelerated Network Technologies Research Group

Martin Žádník

Brno University of Technology, Faculty of Information Technology
Bozetechova 2, 612 00 Brno, CZ
http://merlin.fit.vutbr.cz/ant/

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Motivace

- Security concern (banking, transportation)
- Growing number of attacks

- Internet is open which leads to poor security
- Easier to generate request than to check its validity
- DoS types
  - exhaust server resources (CPU/mem)
  - exhaust network resources (bandwidth)
  - crash the OS or application

DDoS

- Acquire botnets (vulnerabilities, soc. ing.)
- Attack is composed of 2 stages
  - command zombies via IRC
  - zombies attack
- Defense is difficult
  - many sources
  - spoofed sourc.
  - geog. distributed
  - low volumes

Flash crowds

- Large increase of legitimate users' requests
- Differences between DoS and flash crowds

	Bandwidth Attack	Flash Crowd
Network impact	Congested	Congested
Server impact	Overloaded	Overloaded
Traffic	Malicious	Genuine
Response to traffic control	Unresponsive	Responsive
Traffic type	Any	Mostly Web
Number of flows	Any	Large number of flows
Predictability	Unpredictable	Mostly predictable

Internet

- Resource sharing through packet switching
- Best effort
- Simple core and complex edge
  - No authentication ▪ IP spoofing
  - No packet tracing
- Multi-path routing
- Fast Core
- Decentralized management

Attacks

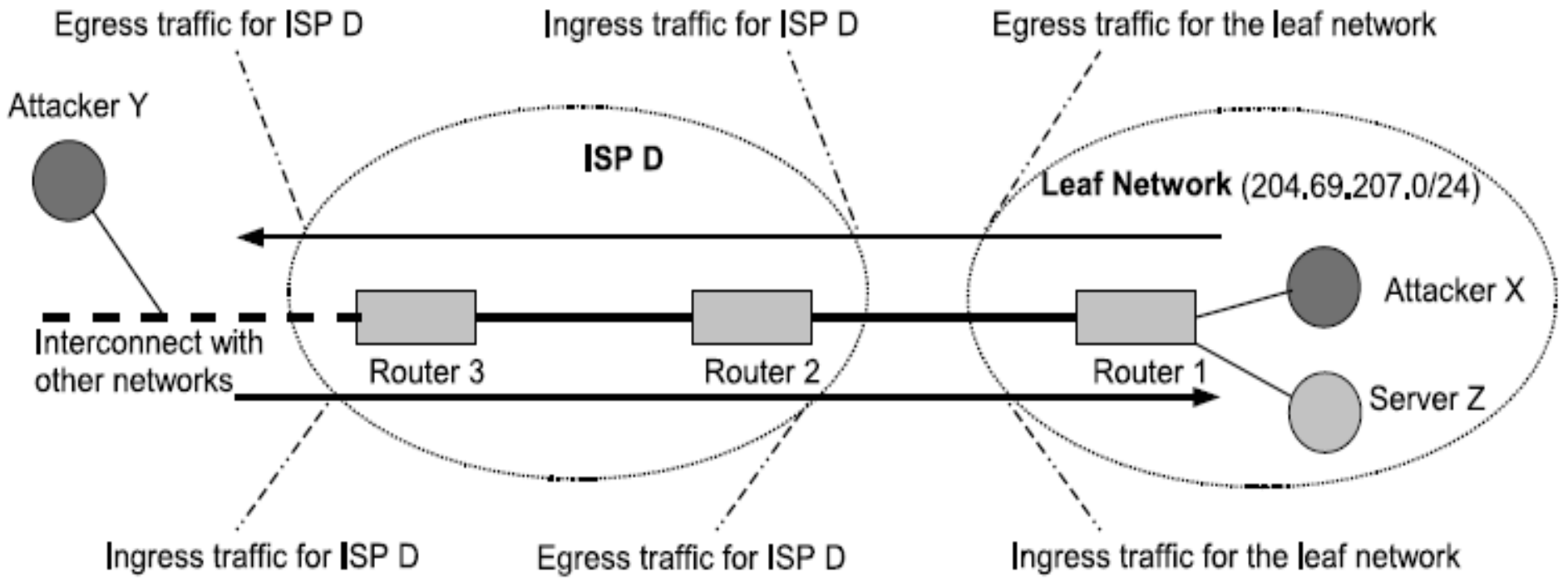
- Metrics
  - packet rate
  - flow rate
  - resource consumption per packet
- Examples
  - SYN flood
  - ICMP flood smurf attack
  - HTTP flood of request
  - SIP flood
  - Distributed Reflector DoS (DNS)
  - Infrastructure attack (on DNS)

Proposed countermeasures

- Attack prevention
  - stop attack before it reaches target
  - close to attacker
- Attack detection
- Attack source identification
  - locate source of attack
- Attack reaction
  - how to filter attack
  - reduce damages

Attack prevention

- Ingress/Egress Filtering
  - pass traffic with IP from expected address range



Ingress/Egress filtering

- Expected IP addresses must be known
- Reverse path filtering
  - problems with asymmetric routing
- Pros
  - mitigate spoofing
- Cons
  - hard to deploy everywhere
  - spoofing is no longer necessary

Router-based packet filtering

- RPF extension of in/egress filtering
  - incorporates BGP protocol
  - to derive set of expected addresses
- If more than 20% of routers implement RPF then the filtering would be successful
- Cons
  - over 2000 AS must adopt RPF
  - BGP modification
  - drop of packet in case of route change
  - spoof on AS network granularity

SAVE

- Source Address Validity Enforcement protocol
  - new routing protocol
  - builds tables of expected IP addresses
  - overcomes asymmetric routing
- Cons
  - difficult deployment
  - spoof only within a subnet

Attack prevention summary

- Solve IP spoofing
- But spoofing is no longer used
- Only 4 out of 1127 attacks used spoofed IP addresses

Attack detection

- Goal is to detect DoS causing a resource consumption rather than semantic attack
- Metric
  - detection time
  - false positive rate
  - portion of attack
- No signature means risk of false positives
- Two types of detection
  - DoS-Attack-Specific detection
  - anomaly based detection

DoS-Attack-Specific detection

- Assumes
  - DoS does not respond to traffic control
  - imbalance in flow rate, packet rate
  - random pattern of sources
  - behaviors at victim and source is
  - correlated

DoS-Attack-Specific detection

- MULTOPS
  - up and down rate unbalance
  - memory attack
- TOPS
  - fixed memory issues by hashing
- Cons
  - up and down rate unbalance is normal
  - could be generated to look normal

DoS-Attack-Specific detection

- Modeling features as random sequence which is homogenous, and changes during attack
- SYN detection – ratio of SYN, FIN, RST
- Batch DoS detection
  - ratio of various parameters UDP, TCP
- Cons
  - the ratio can be arbitrarily generated so
  - the attack can go undetected

DoS-Attack-Specific detection

- Spectral density of packet arrivals
  - assumes attack does not follow TCP flow control
- Cons
  - UDP and ICMP cannot be considered
  - TCP behavior can be mimicked
- CUSUM
  - UDP and ICMP cannot be considered
  - TCP behavior can be mimicked

DoS-Attack-Specific detection

- Summary
  - rely upon particular attack feature
  - difficulties to detect new types of attack

Statistical Anomaly Detection

- Builds normal profile of legitimate traffic
- Assumes that anomaly results in deviation from normal characteristic
- Detect unknown anomalies

- Chi-square tests
- neural networks
- inspiration by immune system

- processing speed, accuracy, false pos.

Attack source identification

- Backscatter traceback
  - Sinkhole router for unallocated IP addresses monitors which port DoS arrived
- CenterTrack
  - Overlay network with routers capable of tracking
- Cons
  - Participating routers
  - Does not work if addresses are valid
  - Overhead

Probabilistic IP Traceback

- PPM – probabilistic packet marking
- – routers insert with a certain probability
- info about the partial path into the packet
- (adjusted to router's distance)
- iTrace
  - routers sends ICMP info to destination

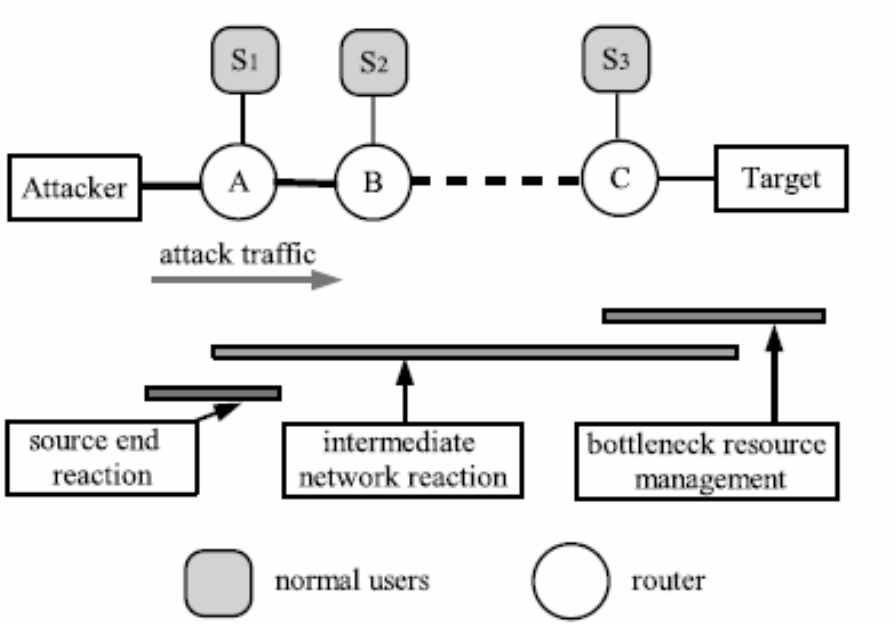
- Cons
  - overhead
  - authentication
  - low volume, hence no marking

Hash-based IP Traceback

- Bloom filter on every router interface
- Traceback query collects the path
- Cons
  - new protocol
  - modification of routers

Attack reaction

- Bottleneck resource management
  - host-based management
  - network management
- Resources should be managed up to the attacker, otherwise waste of resources



Host-based management

- Modify OS
  - fig bugs
  - SYN cookies
  - SYNkill
- Decrease traffic rate
  - traffic shaping CBQ
- Increase processing power
  - load balancing
- IP filtering based on known IP database

Host-based management

- Pros
  - easy to implement
  - most commercial solutions
  - costly
- Cons
  - need to classify traffic into classes
  - treat classes differently
  - DDoS can be classified as legitimate

Intermediate network reaction

- Performed by routers in between
- Pushback mechanism
  - ask adjacent router to filter based on victim's ID
- Agent-controller
  - ask source routers to mark packet and derive which router is an entry point
- Cons
  - message may be dropped
  - overhead
  - authentication

Intermediate network reaction

- Secure overlay network (SOS)
  - traffic is verified by access point
  - sent to a beacon node selected by hash
  - forwarded to servlet
  - target selects which traffic to receive
- Pros
  - distributed firewall
  - unknown link to victim
- Cons
  - new routing protocol
  - deployment of access points

Secure overlay network (SOS)

- traffic is verified by access point
- sent to a beacon node selected by hash
- forwarded to servlet
- target selects which traffic to receive
- Pros
  - distributed firewall
  - unknown link to victim
- Cons
  - new routing protocol
  - deployment of access points

Source end reaction

- D-WARD
  - compares traffic model at the source
  - if deviation then rate limit at the source

- Cons
  - for DDoS the deviation at the source can be small
  - ISP has no motivation to implement

Integrated solution

- Pushback
- Challenge admission request on demand via proxy

- Implemented in distributed manner
- Issues
  - how to implement pushback
  - how to implement challenge

Summary

- Combination of various proposals
- Bad legislative background