Defending against Flooding-based Distributed Denial-of-Service Attacks: A Tutorial

AUTHOR ROCKY K. C. CHANG, THE HONG KONG POLYTECHNIC UNIVERSITY

PRESENTED BY CHUNG TRAN

Outline

- Introduction
- DDoS history
- DDoS type of attacks
- Solutions
- Firewall
- Four detect and Filters approaches
- Conclusion

Introduction

- In a typical DDoS attack, a large number of compromised hosts are amassed to send useless packets to jam a victim, or its internet connection, or both.
- ICMP Flood, Smurf attack, Ping flood, and Ping to death
- SYN Flood
- Teardrop Attack
- Etc etc.

Introduction cont.

- Can be accomplish by:
  - By pinging to death
  - Computational intensive tasks on the victim such as Encryption and Decryption of data
  - Many differences flooding types of attack

History Part 1

- 1989- First ICMP/Ping floods
  - First occurrence of the –f(flood) of the ping.c source code
- 1990-The first homeland of DDoS
- 1996 September – First high profile DDoS attack
- 1996 September – First CERT DDoS Advisory
- 1997 – First Publicly Available DDoS Tool Released
- 1997 – DDoS attacks morph

History Part 2

- 1997 - ICMP / Ping floods grow
- 1999 July – DDoS attacks expand
- 1999 October – Industry expects combine to address DDoS threats
- 1999 December - DDoS hit mainstream media
- 1999 December – US Government takes note of DDoS
- 2000 February – 15 year old boy shows how easy DDoS attack can be

History Part 3

- 2001 – CERT warns of trend in self-propogating worms
- 2001 – Attacks grow from Mbps to Gbps
- 2002 – Scope of DDoS attacks expands
- 2003 December – Barrett Lyon founds company to defend organizations against DDoS attacks
- 2004 – Online payment systems attacked
- 2005 December – Extortion schemes Expand

History Part 4

- 2006 December – Small scale DDoS attacks from religios groups
- 2007 December – State sponsored DDoS attacks cripple a small nation
- 2013 – DDoS attacks Exceed 150 Gbps
  - Largest recorded DDoS attack size reaches a new unprecedented level: Two high profile attacks recorded above 150 Gbps in the first half of the year

DDoS attacks

- There are many types of attacks as the years progress DDoS have become more complex
- This paper break it down into 2 type of attacks direct versus reflector
- Direct Attack: an attacker arranges to send out a large number of attack packets directly toward a victim
  - Can be a combination of TCP, ICMP, and UDP
- Reflector attack: is indirect attack in the intermediary nodes routers and server

DDoS type of Attacks

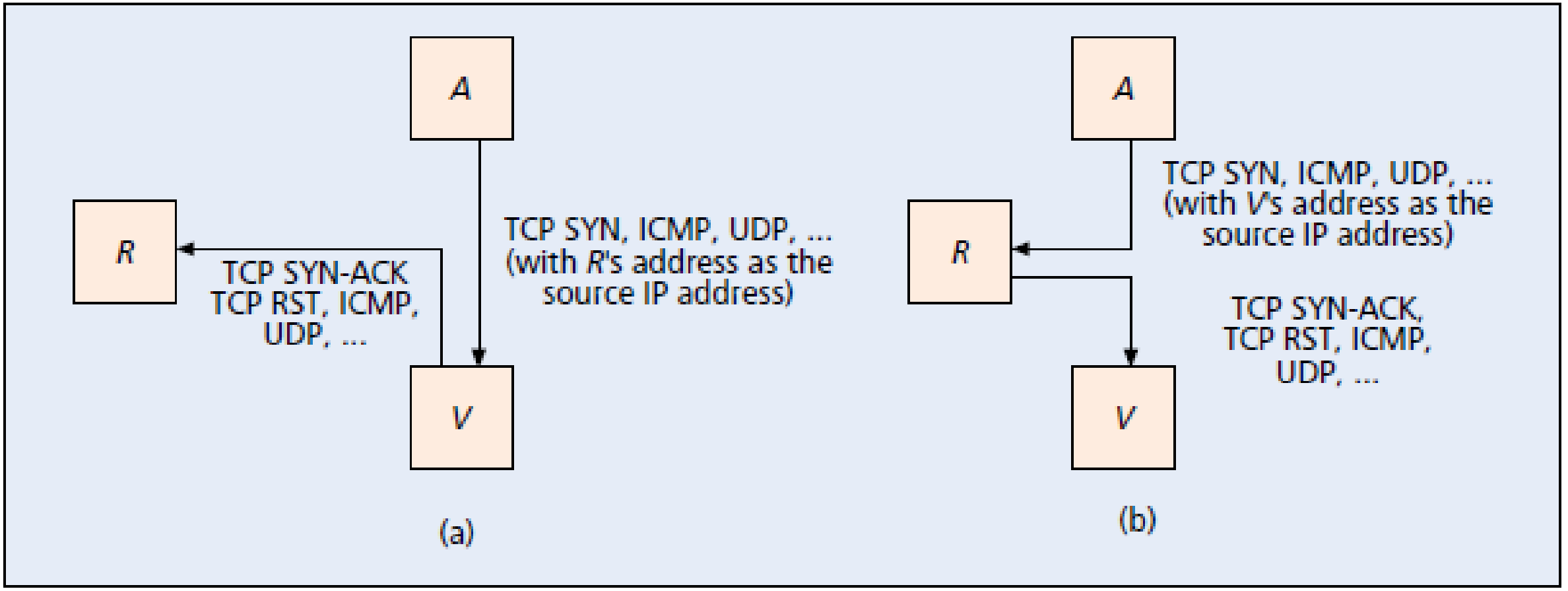


Figure 1. *Two types of flooding-based DDoS attack: a) direct; b) reflector.*

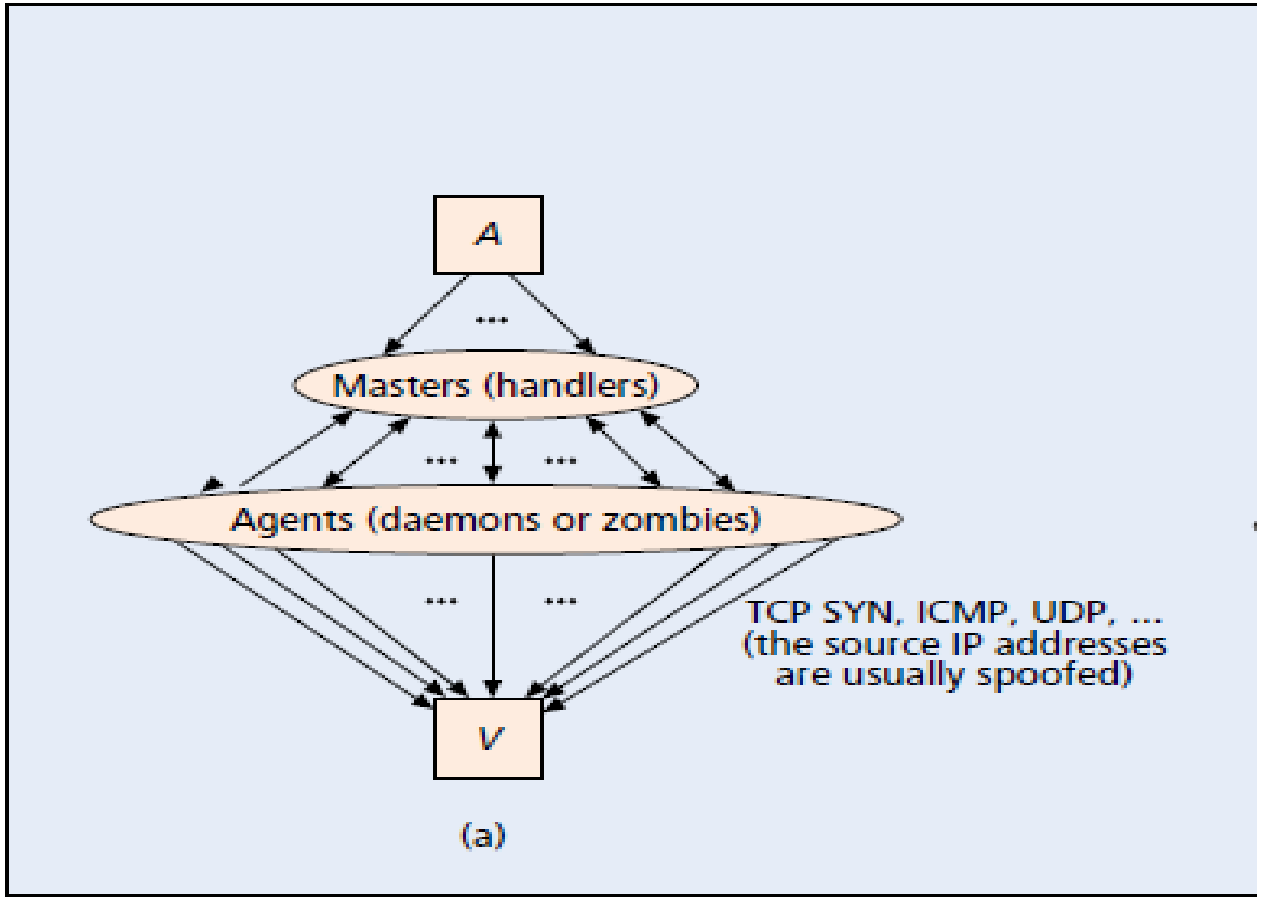
Direct attack

- As the diagram show the advisory send packets to the victim directly using TCP, UDP, and ICMP
- A router and server is not part of the attack
- This can often be call peer-to-peer attack

Reflector Attacks

- The advisory set it up and place the DDoS attacks on the routers and server for victim to visit and get attack from it
- This build up until there is large enough reflectors from routers and server for a flood to happen causing the victim systems compromise

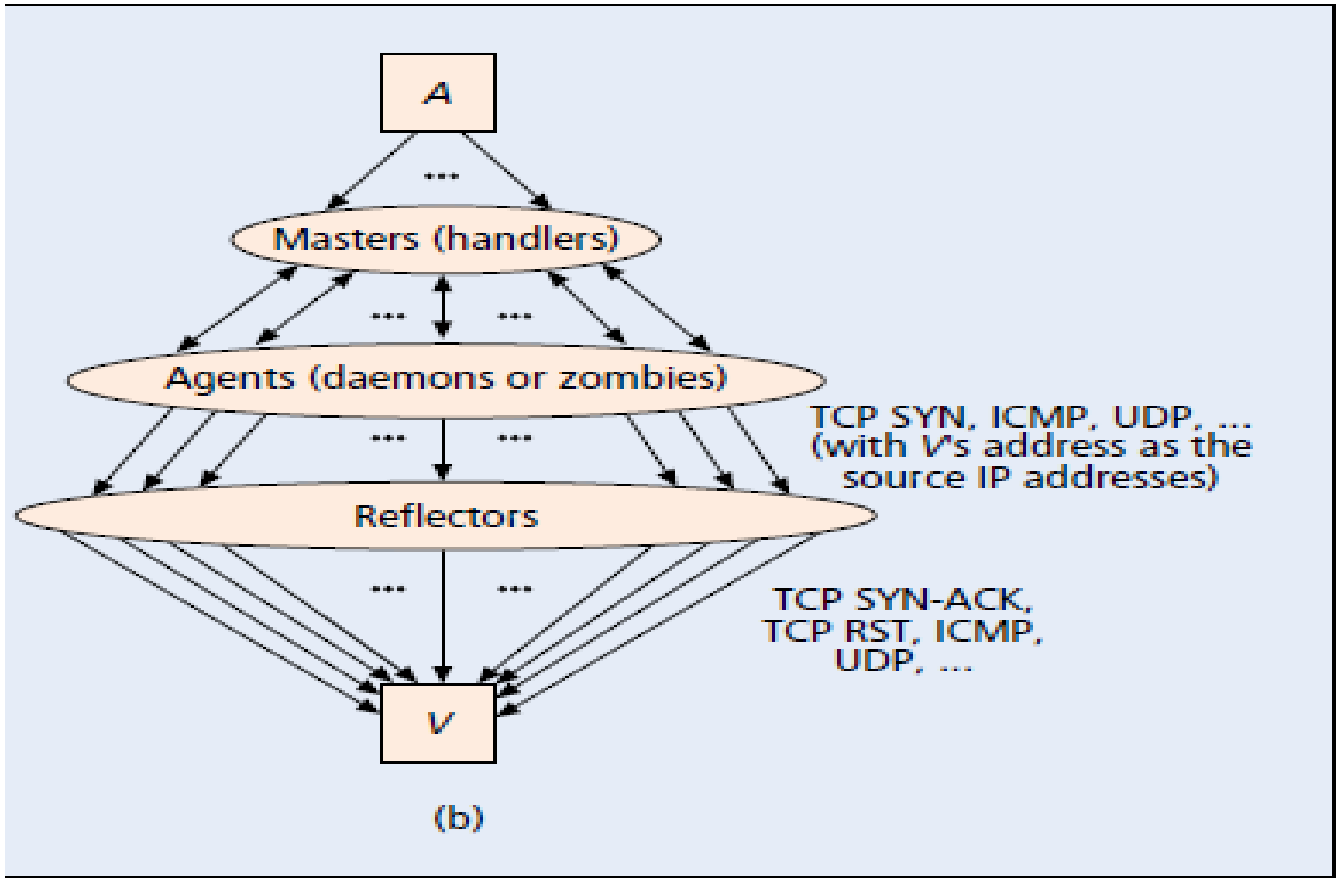
Attack Architectures for Direct attack



Architect of Direct Attack

- The Attacker setup many other hosts these are call daemons or zombies
- As the victim system become compromise the victim can and often become a new daemon or zombie and attack the next victim
- As more computers are network this effect can grow very fast this is why we having over Gbps recorded attack

Architect of Reflectors Attack



Architect of Reflectors Attack

- Not much different but the zombies and daemons send the attack packets to routers or servers before it attack the victim
- The most important part to remember is that the routers and servers are often innocently uses as part of the attack
- The attackers set the inscribed source destination to the victim destinations

Some Reflectors attack

	Packets sent by an attacker to a reflector (with a victim's address as the source address)	Packets sent by the reflector to the victim in response
Smurf	ICMP echo queries to a subnet-directed broadcast address	ICMP echo replies
SYN flooding	TCP SYN packets to public TCP servers (e.g., Web servers)	TCP SYN-ACK packets
RST flooding	TCP packets to nonlistening TCP ports	TCP RST packets
ICMP flooding	• ICMP queries (usually echo queries) • UDP packets to nonlistening UDP ports • IP packets with low TTL values	• ICMP replies (usually echo replies) • ICMP port unreachable messages • ICMP time exceeded messages
DNS reply flooding	DNS (recursive) queries to DNS servers	DNS replies (usually much larger than DNS queries)

SYN Flooding

- There is a three-way handshake for TCP
- A SYN flood attack works by not responding to the server with the expected ACK code
- Not sending the excepted ACK, or by spoofing the source IP Address from the SYN
- This cause the server to send SYN-ACK to falsified IP address – which will not send an ACK because it "knows" that it never sent a SYN

SYN Flooding cont.

- The server will wait for the ACK for some time this wait due to a possible network congestion
- In an attack increasing large numbers of half-open connections will bind resources on the server until no new connection can be made, this cause Dos
- Here is a simple way to see it

SYN flooding queue

- G/D/∞/N
- N – half open connection
- G – General arrival rate of the SYN Packets
- D – Deterministic lifetime of each half-connection from the three-way handshake
- It continue to uses up the resource available waiting for the complete three-way handshake that will not come in an attack so it keep expending the connections

Graph of a Syn Flooding

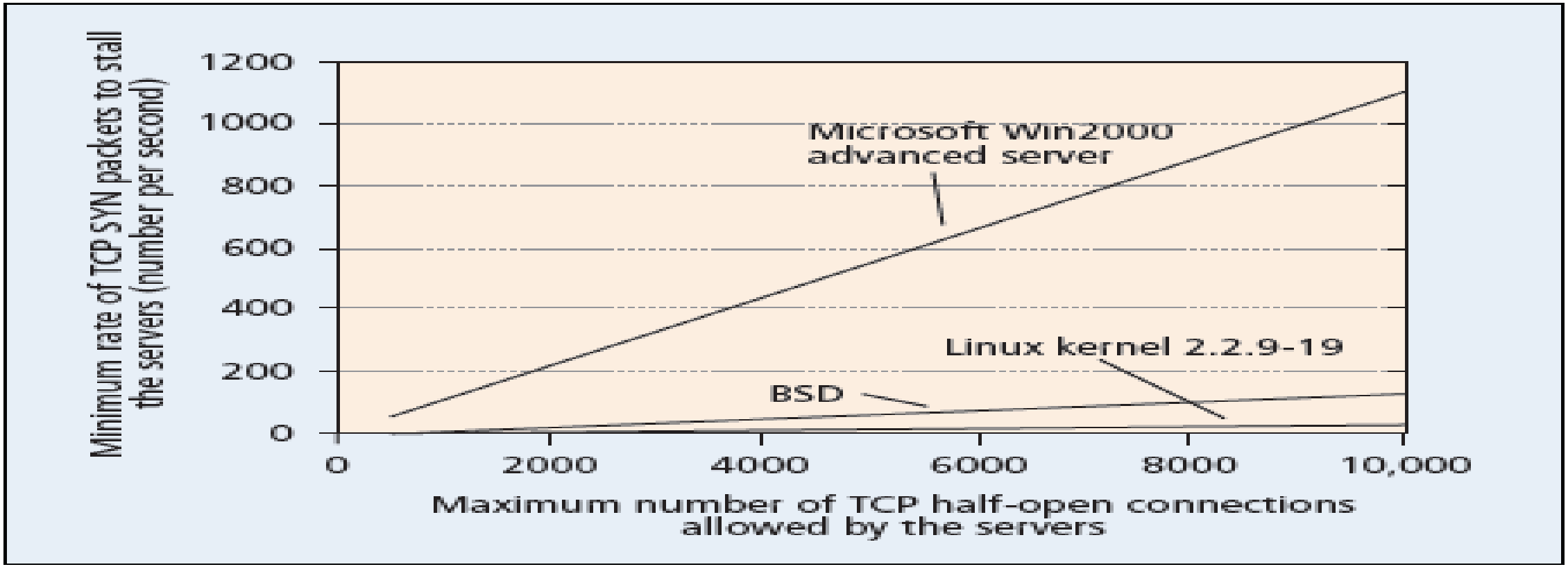


Figure 3. ***Minimal rates of SYN packets to stall TCP servers in SYN flooding attacks.***

Analysis of the Graph

- It show that in the graph that when N <= 6000 both BSD and Linux will stall at 56 kb/s
- At 1Mbps N <= 10000 for all 3 to stall
- Windows system does the best in SYN flooding attack

Solution to DDoS Problems

- Three lines of defense:
  - Attack Prevention and Preemption (before the attack)
  - Attack Detection and Filtering (during the attack)
  - Attack Source Traceback and Identification(during and after the attack)

Best is to uses all 3 in a system against DDoS type of attack

Attack Prevention and Preemption

- Passive side: protect hosts from master and agent implants by using signatures and scanning procedures to detect
- Monitor network traffic from known attack message sent between attackers and masters
- Active side: employ cyber-informants and cyber-spies to intercept attack plans(group of cooperating agents)

By itself is not enough once an attack have happen this method cannot stop the attack

Traceback and Identification

- After an attack or during an attack
- IP traceback: Identifying actual source of packets relying on source information
  - Routers can record information they have seen
  - Routers send addition information to destination or on another channel, ICMP message

Traceback and Identification

- IP Traceback not always possible:
  - Cannot always trace a packets to the origins(NATs and firewall)
  - IP Traceback also ineffective in reflector attacks

If traceback was possible than those individual responsible can be put away

Detection and Filtering

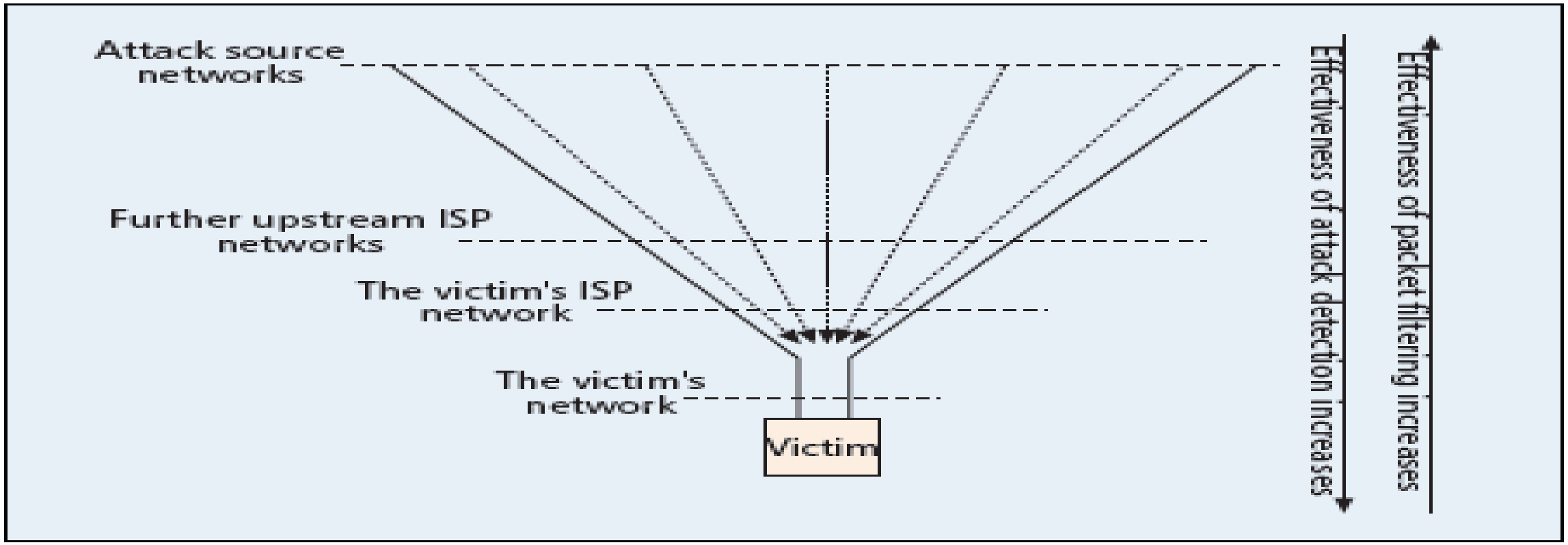


Figure 4. *Possible locations for performing DDoS attack detection and filtering.*

Detection and Filtering

- 2 Parts
  - Detection: Identifying DDoS attack packets
  - Filtering : Classifying packets and dropping them

- Effectiveness of Detection
  - FPR(False Positive Ration) # of false positive/Total # of confirmed normal
  - FNR (False Negative Ratio) # of false negative/Total # of confirmed attack packets

Detection and Filtering cont.

- Effectiveness of Filtering
  - Referring to the level of normal service that can be maintained by the victim during a DDoS attack by filtering the attack packets
  - Effective attack detection not always translate into effective packet filtering
  - Can be measured by normal packet survival ratio(NPSR) How many normal packets make it to the victim during a DDoS attack

Detection and Filtering

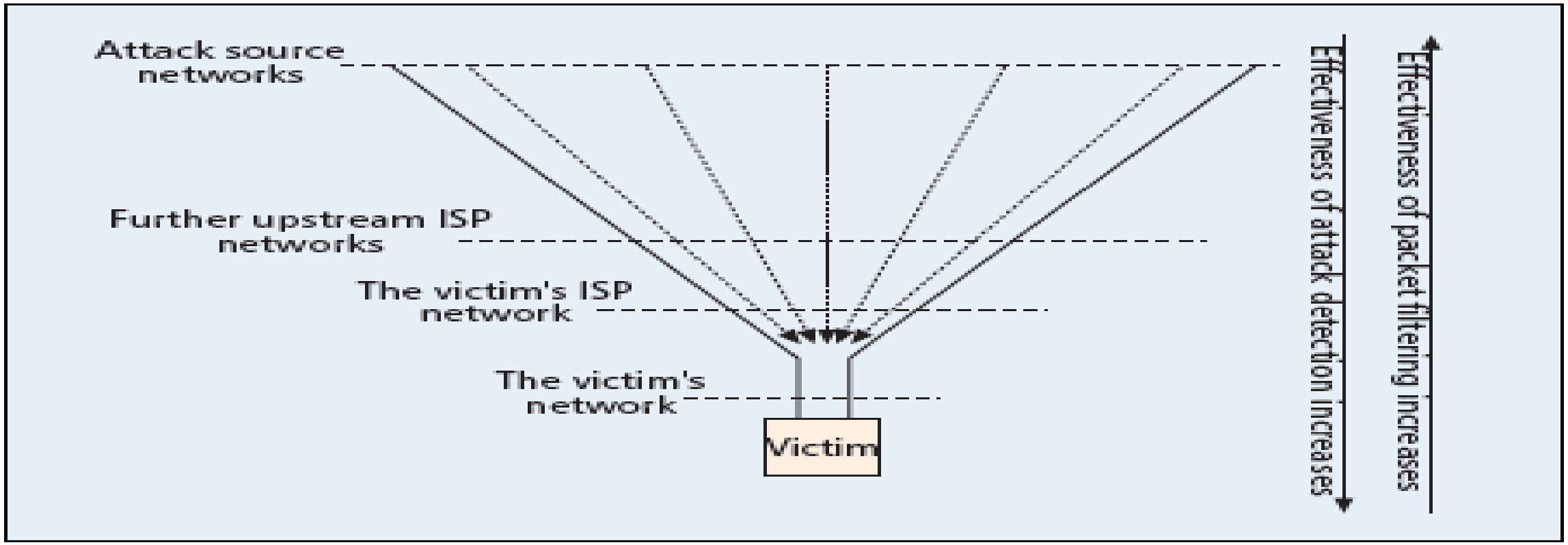


Figure 4. *Possible locations for performing DDoS attack detection and filtering.*

Source Network

- Often cannot detect but can filter out attacking packets by checking spoofing IP address
- Direct attack easy to track reflector attacks much more difficult
- Make sure all ISP networks on the Internet, was impossible when paper came out

Third points are being work on. This is due to fact that such a high volume of attack have occur in the last few years 150 Gbps first half of 2013

Victim's Network

- Victim can detect a DDoS attack based on an unusually high volume of incoming traffic or degraded server and network performance
- Commercial products can be obtain for this purpose, EMERALD was mention in this paper when it came out
- Other defensive that does not uses detection and filter have been suggested i.e. IP hopping, moving target defense change of IP address so the attacker cannot keep using your spoof address to attack

Victim's Upstream ISP network

- Victim's request filter packets
- Well design or else good packets can be drop
- Automated to detect intrusion in an alert systems
  - Careful design in case of TCP, victim network will not receive acknowledgements in midst of an attack.
  - Use strong authentication and encryption

Further upstream ISP network

- Extend all of the approached mention
- This require the victim's network to detect DDoS attacks
- Once detected the upstream ISPs are notified to filter attack

I know this all sound like a lot of work but with so many attacks occurring and rising what choice do we have but to be conscious of it

Internet Firewall

- Propose an Internet firewall to protect the whole Internet was made
- Idea is to detect it on the internet and drop it before it can reach a victim network
- 2 Approach:
  - route-based packet filtering approach
  - Distributed Attack detection Approach

Route-Based Packet Filtering Approach(RPF)

- This idea was propose by Park and Lee
- Distribute packet filterings to examine whether each received packet come from a correct link base on source and destination address
- If received from an unexpected link it then dropped
- However, a packet might still be legitimate because there might have been a route change
- No good against Reflectors attacks

Distribution Attack Detection(DAD)

- Second Internet firewall Approach
- DAD approach detects DDoS attacks based on network anomalies and misuses observed from a set of distributed detection system(DSs)
- Detect normal traffic pattern versus “significantly” deviate from the normal ones.
- Base on known attack pattern

DS Design consideration

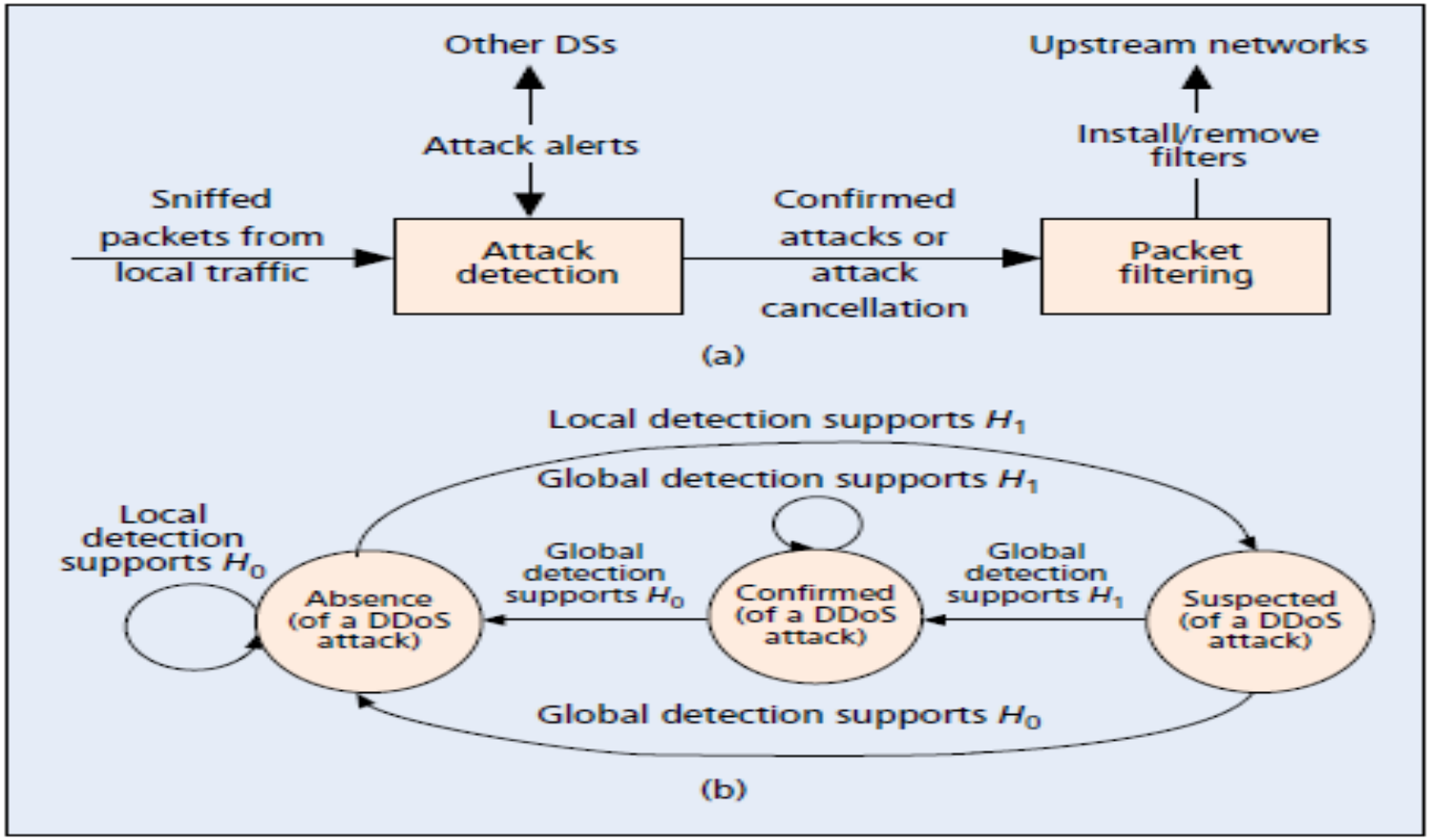


Figure 5. *a) High-level DS architecture and b) a state diagram of two-level attack detection in the distributed detection approach.*

DS design consideration

- Need to process packets at very high speed as shown in the diagram before
- Each DS can only observe partial traffic anomaly
- This is where we have two levels: *local detection* and *global detection*
- H1 for presence of DDoS attack
- H0 a null hypotheses

Binary Hypothesis

- Test a set of packet flows
  - Share same destination IP address
  - Packet types
  - TCP flags
  - Port number

Slow down network especially during an attack do suggest just install on known and confirm attack switches. Running out of time so I must cut this short over 45 minutes of presentation already

Conclusion

- With the very first attack occurring in 1989 DDoS have taking off and change over the years
- There been many suggested way to prevent attacks
- There are the Preemptive/Prevention approach, Traceback/identification, and Detection/Filtering most of this seems to have problem with Reflectors type of attack
- More research are in development for this problem

Personal comments

- I know there a lot of research out there trying to stop DDoS, but seeing the number make me think that it a losing battle.
- In the last decade alone there been report of attack on every accept of our infrastructure; financial, media, government, social, etc.
- Is this a losing battle for personal privacy?
- Comments?