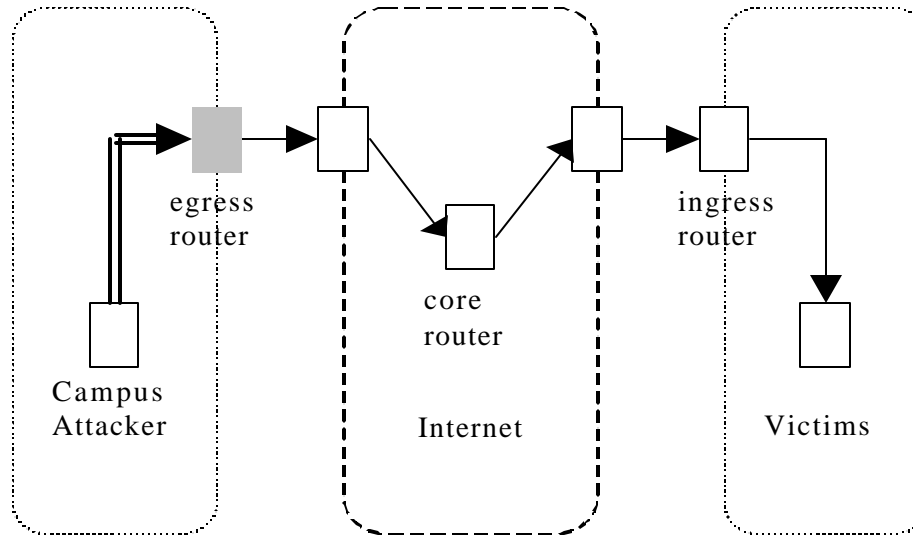


IP Traceback

Denial Of Service

- Some DOS attacks succeed through spoofing.
- If packets are filtered at network ingress for spoofing
 - Easy to catch the attacker
 - Consequent penalties will deter attackers
- Can control DOS attacks

Ingress filtering



DOS attacks

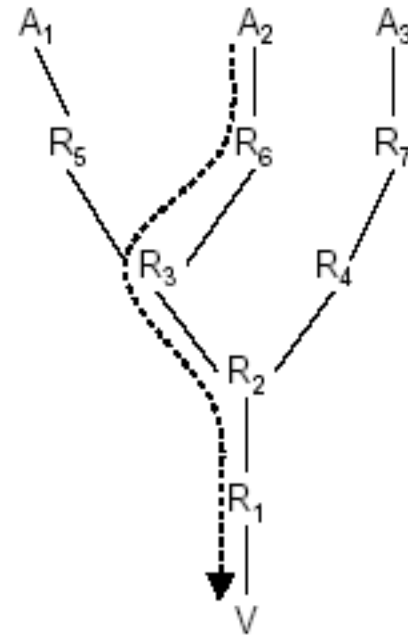
- Ingress filtering is not widely employed
 - Can be expensive in transit and backbone networks
- How to effectively trace back the source of the attack?
- If successful, may be able to throttle attack traffic at the network ingress

I CMP traceback(Bellovin, IETF)

- Generate I CMP packets with packet header, router and its neighbors ids
- Do this with low probability $1/20,000$
- These I CMP packets can be used to trace the source
- More likely to get packets from routers closer to destination, rather than source

IP traceback (Savage...Sigcomm00)

- Exact Traceback
 - R_6, R_3, R_2, R_1
- Approximate Traceback
 - Valid path suffix
 - R_5, R_6, R_3, R_2, R_1



IP traceback -assumptions

- Attacker can generate any packet
- Attackers may conspire
- Aware of the tracing mechanism
- Attackers send lots of packets
- Packets may be lost, reordered
- Routes are pretty stable
- Routers are memory, CPU limited

IP traceback –Node Append

- Attach each router's IP address to the packet
 - Like IP record route option
- Every packet will have path info
- Too expensive
- Could lead to fragmentation problems

Node Sampling

- Reserve a node field
- Routers write their IP address with probability p
- Prob. Of receiving id from d hops
 - $p(1-p)^{d-1}$
- $p > 0.5$, robust against attacker spoofing
- Routers far away from victim don't send many packets
 - $d=15, p=0.51, \text{expectation} = 42,000 \text{ packets}$

Edge Sampling

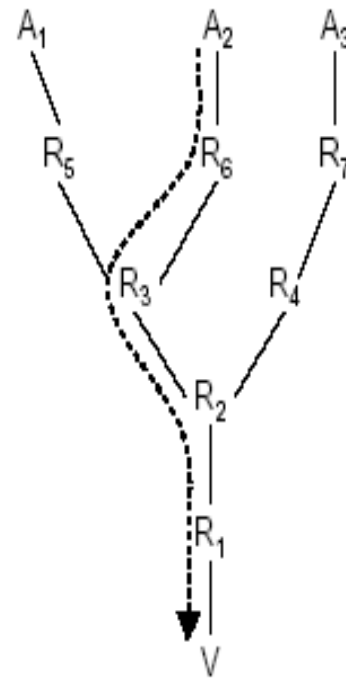
- Encode edges of path
 - Rather than single nodes
- Employ three fields
 - Start, end, distance
- With probability p , write Router IP address in start, make distance =0
- Else, (a) if start already marked, distance=0, put your id in end and
 - (b) increment distance

Edge Sampling

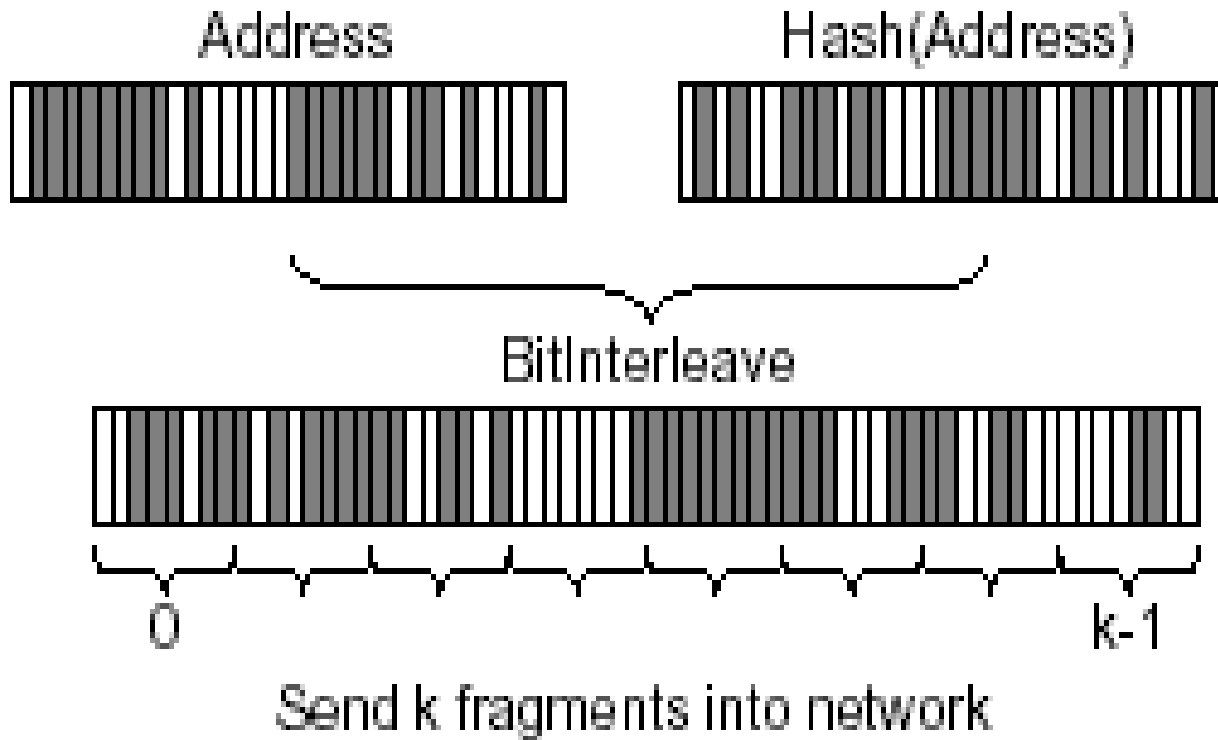
- Tree construction starting from victim (distance =0, 1,...)
- Time for convergence
 - furthest router: $p(1-p)^{d-1}$
- Can use any p , spoofed attacker packets distance field longer
- Robust against multiple attackers
 - Edges are different, linear complexity
- Takes many bits - $32+32+8? = 72$

Edge Sampling --encoding

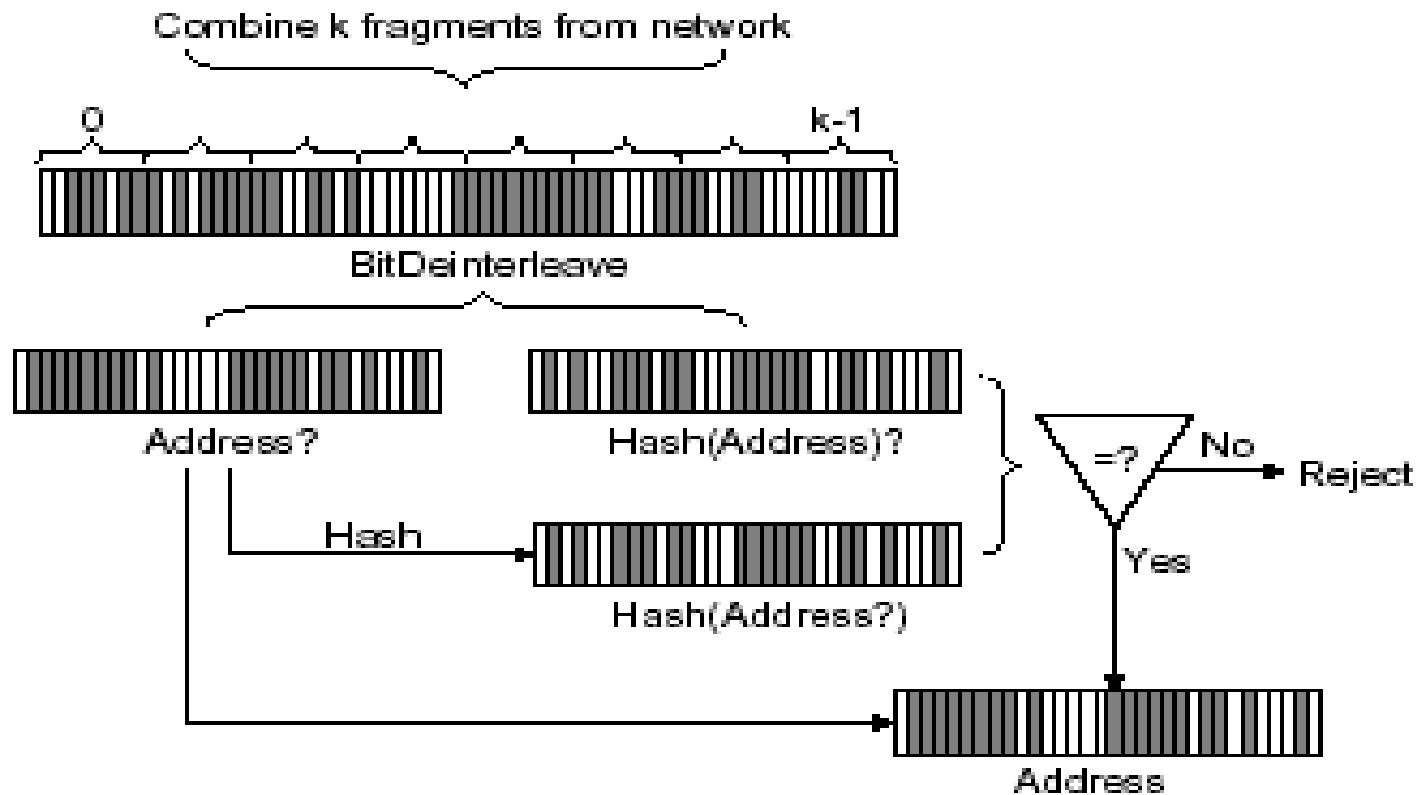
- Use XOR of addresses
- $R_1, 0$
- $R_1 \text{ XOR } R_2, 1$
- $R_1 \text{ XOR } R_2 \text{ XOR } R_3, 2$
- Uses roughly half the space



Edge Sampling— Fragment Sampling



Fragment Sampling



Fragment Sampling

- Can compress information into 16 bits
- Use IP fragment identifier space
- Expensive to compute
- Not robust against large DDOS

Advanced Marking Scheme

Song & Perrig, Infocom01

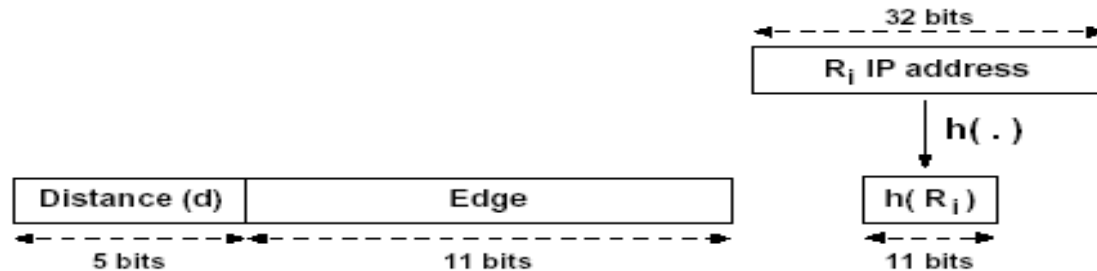
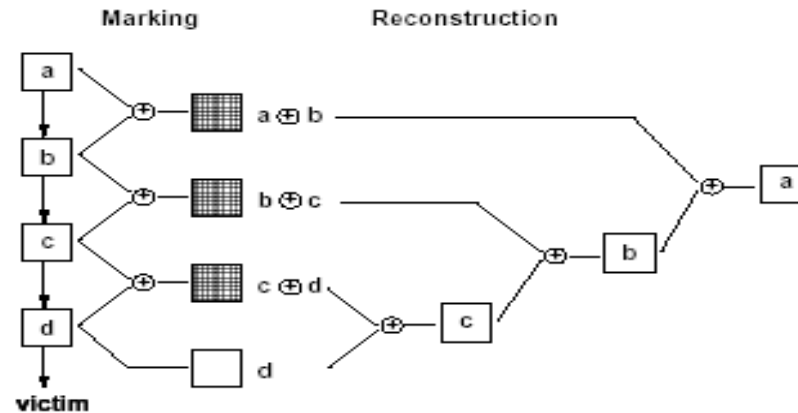


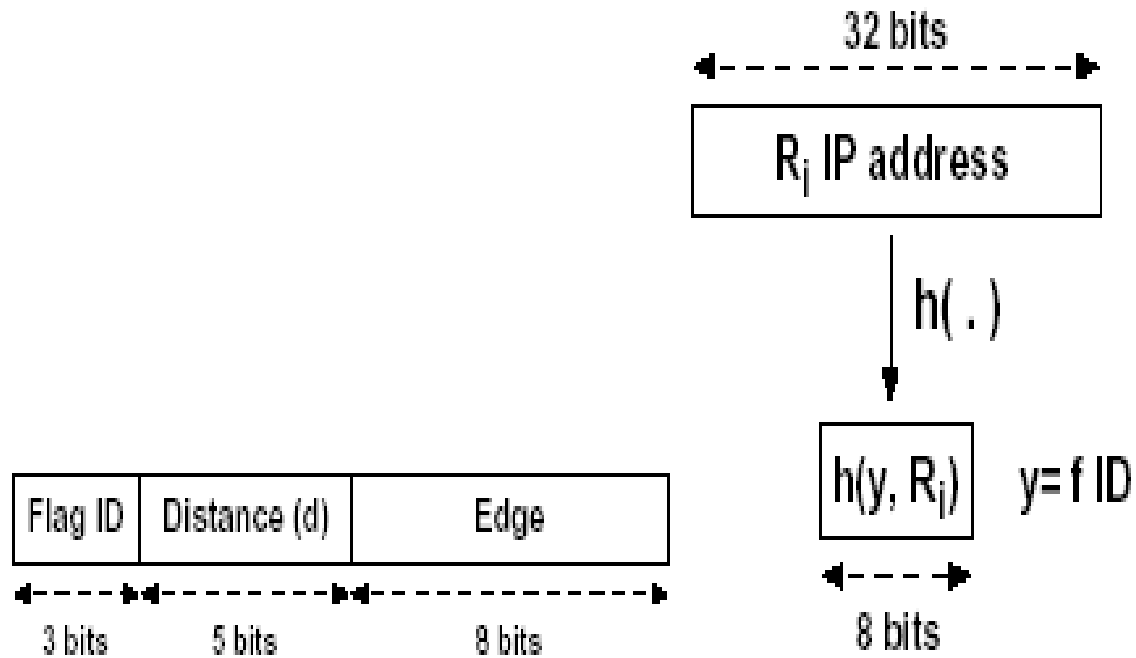
Figure 2: Encoding in Advanced Marking Scheme I



AMS

- Use two hash functions h and h'
- Encode $h(\text{start}) \text{ XOR } h'(\text{end})$
- Use 11-bits for hash, 5bits for length
- If you know upstream routers, few choices for $h(s)$, when we know $h'(e)$
- Tolerate multiple attackers
 - Upto 60
 - Main limitation: hash collisions

AMS-II



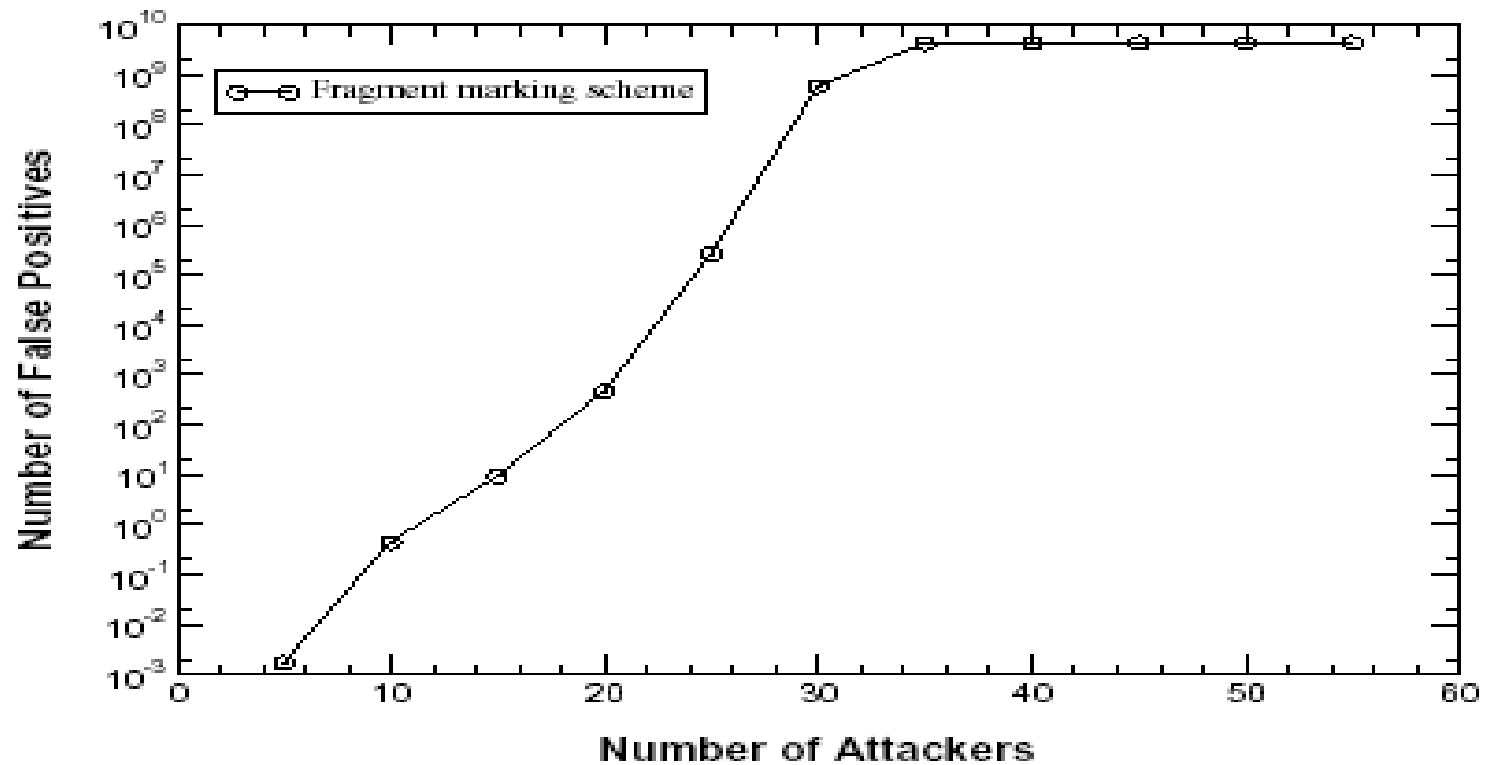
AMS-I I

- Use two sets of hash functions
- Main intuition:
 - Probability of collision with 11 bits $1/2^{11}$
 - Probability of collision with m hashes of 11 bits = $1/(2^{11})^m$
 - Multiple hash functions reduce Collisions
- Where did we see that before?

AMS-II

- Tries to work within the space of 11 bits
 - While identifying the hash function
- Easier than FSM
- Much more robust than FSM

FMS False positives



AMS & AMS-II

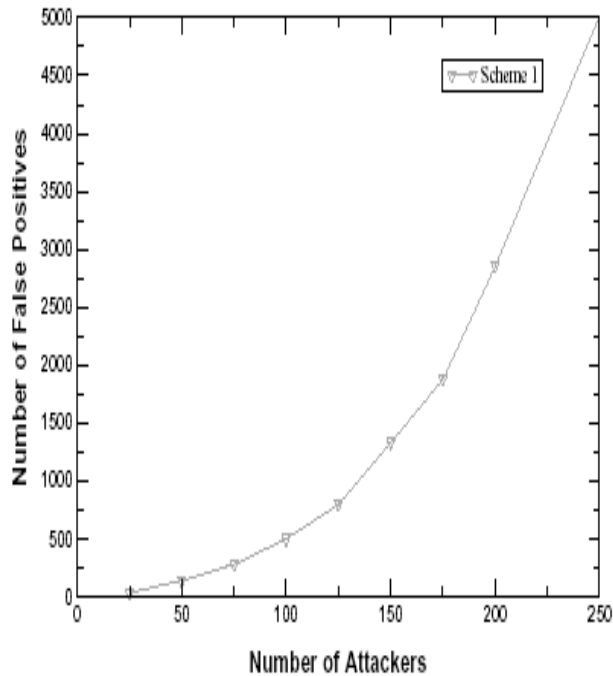


Figure 7: False Positives for Advanced Marking Scheme I

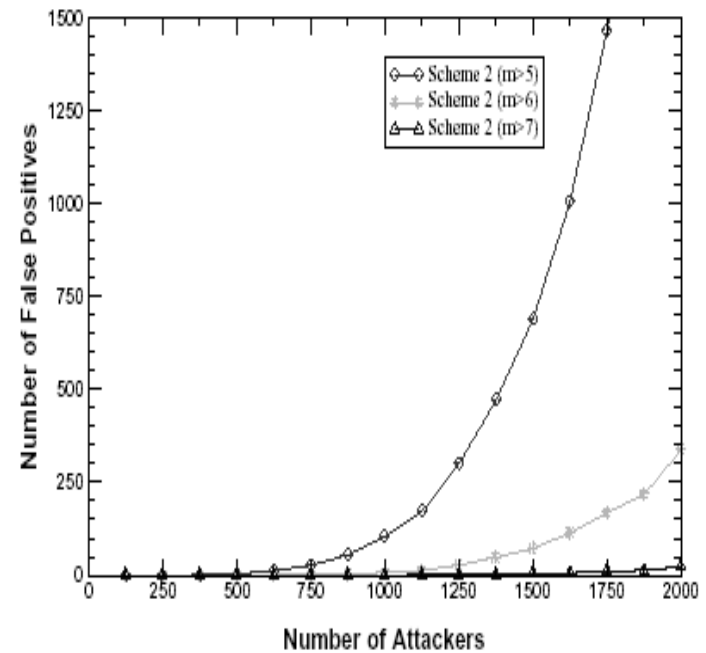
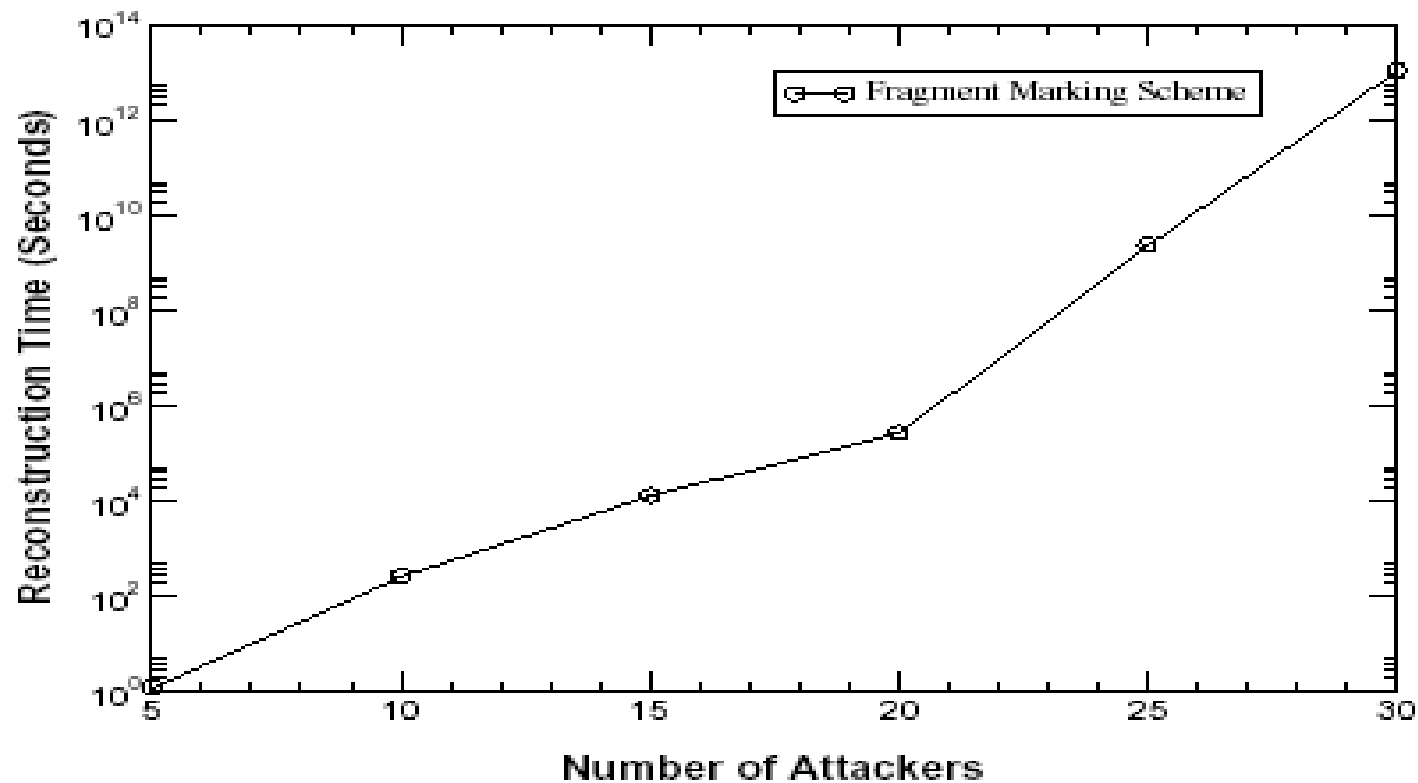
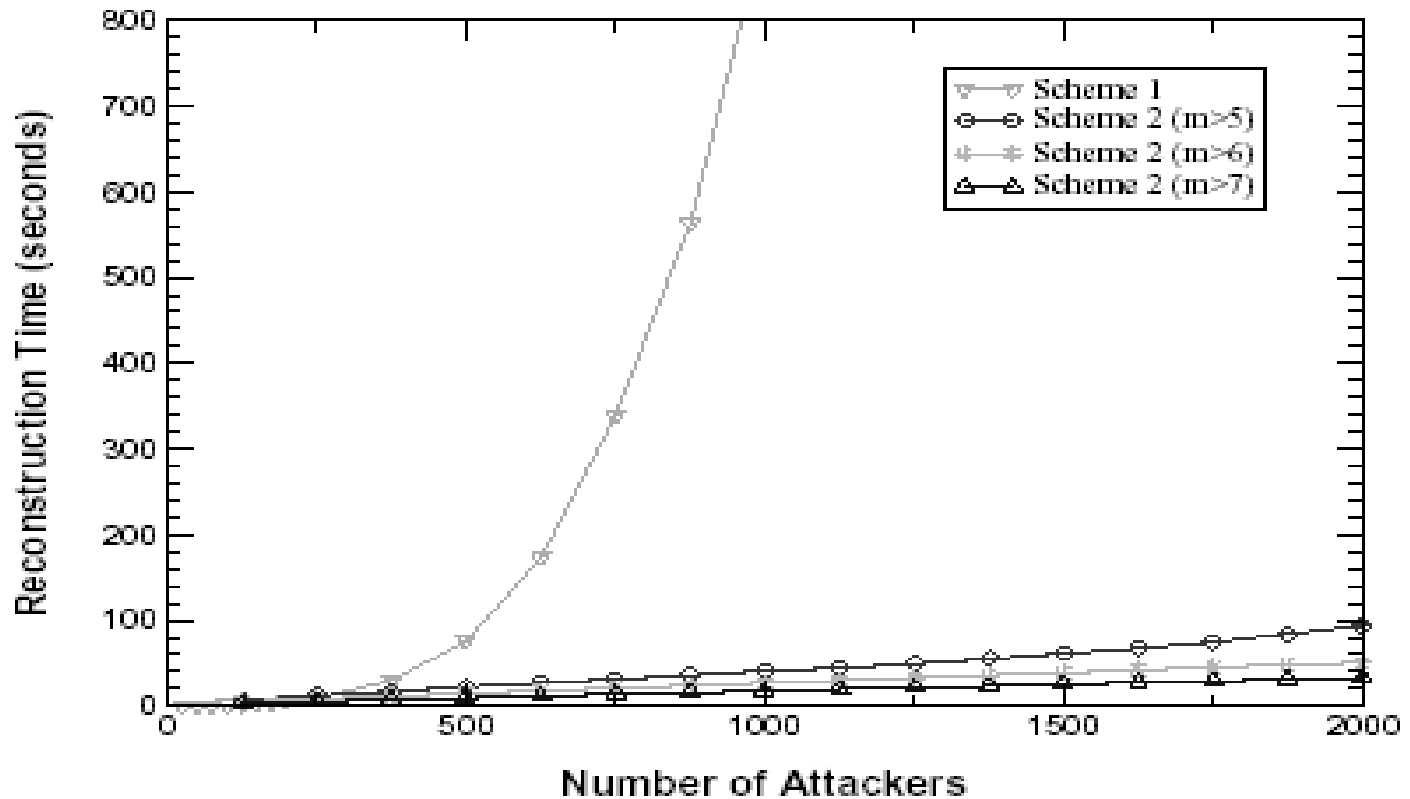


Figure 8: False Positives for Advanced Marking Scheme II

FMS Path reconstruction time



AMS Path Reconstructin times



Traceback features

- Information travels with attack packet
 - Will take the same path as attack
 - May not be with ICMP traceback
- Packet unlikely to be filtered
- Assumes Fragmentation field available
 - Not present in IPv6, at times encrypted

Summary of today's class

- Traceback is an interesting idea
- Allows us to trace the origin of the attack
- Threat of Identification leads to reduction in attacks
- What about the viruses?
 - Innocent attackers
 - Raised the bar for a DDOS attack

References

- [1] Savage et al, "Practical Network support for IP Traceback", ACM Sigcomm 2000
- [2] Song, Perrig, "Advanced Marking Schemes", Infocom 2001.