

IP Traceback

Mobin Javed

Overview

- Will discuss in detail the paper,
“Advanced and Authenticated Marking Schemes for
IP traceback”
(INFOCOM 2001)
- Briefly touch upon follow-on papers.

Design Requirements

- Efficient
- Accurate
- Authenticated markings

Advanced Marking Scheme I

- If the victim has a map of its upstream routers, full edge ID is not required to be communicated.
- Only a hash value of the ID can be marked in the packet.
- *Remember efficiency problem was arising due to “fragments”.*

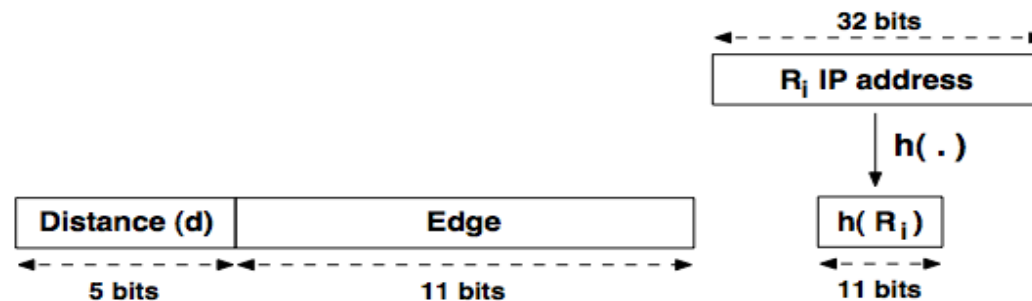


Fig. 2. Encoding in Advanced Marking Scheme I

Theoretical Analysis

- Number of packets required in reconstruction
1/8th of the no. required by FMS scheme
- False positives
 - Can still arise due to collisions in hashes.
 - For more than **60** distributed attacker sites, 11 bit hash value is not sufficient.

Advanced Marking Scheme II

- We want more accurate results – i.e. reduce false positives.
- Instead of one hash functions, use a **set** of hash functions.
- Intuition: probability of same hash value for two routers using,
One hash function - $1/2^{11}$
m hash functions - $1/2^{11 \cdot m}$

Advanced Marking Scheme II

- How to determine which hash function should the router use?
- Also during reconstruction, victim needs to know which hash function router used to mark each packet.
- Solution : use a flag ID

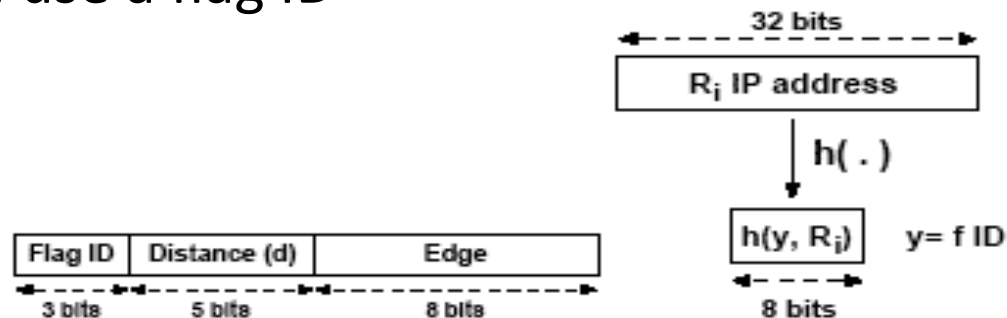


Fig. 5. Encoding for Advanced Marking Scheme II

Advanced Marking Scheme II

- To reduce false positives use an m -threshold scheme in reconstruction.
- If more than m hash variations of a router match the markings in the attack packets, consider it to be on attack graph.
- Else, it was a false positive.

Simulation Results: False Positives

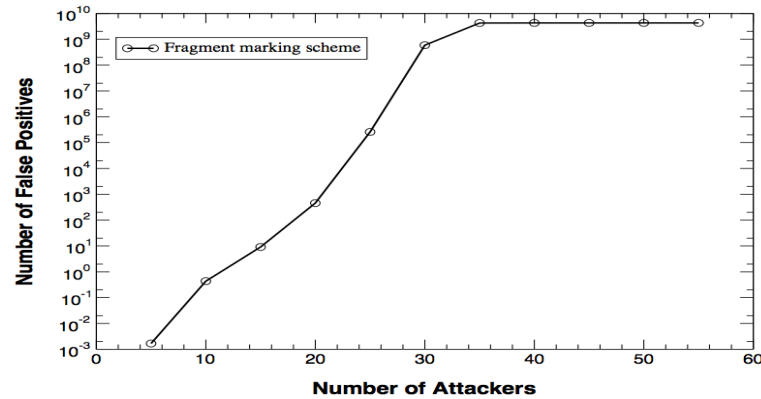


Fig. 10. False Positives for FMS

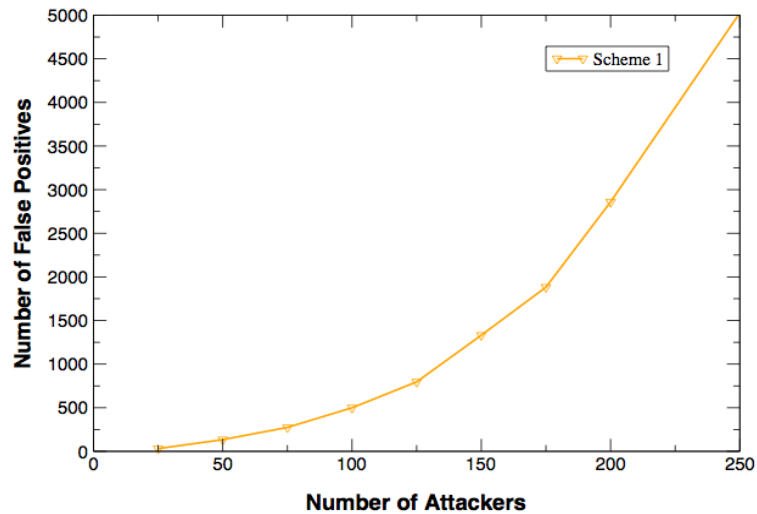


Fig. 7. False Positives for Advanced Marking Scheme I

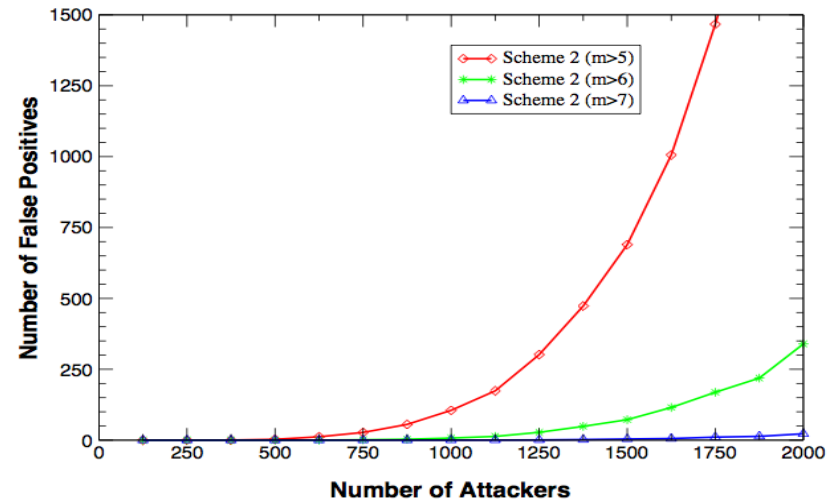


Fig. 8. False Positives for Advanced Marking Scheme II

Simulation Results: Reconstruction Time

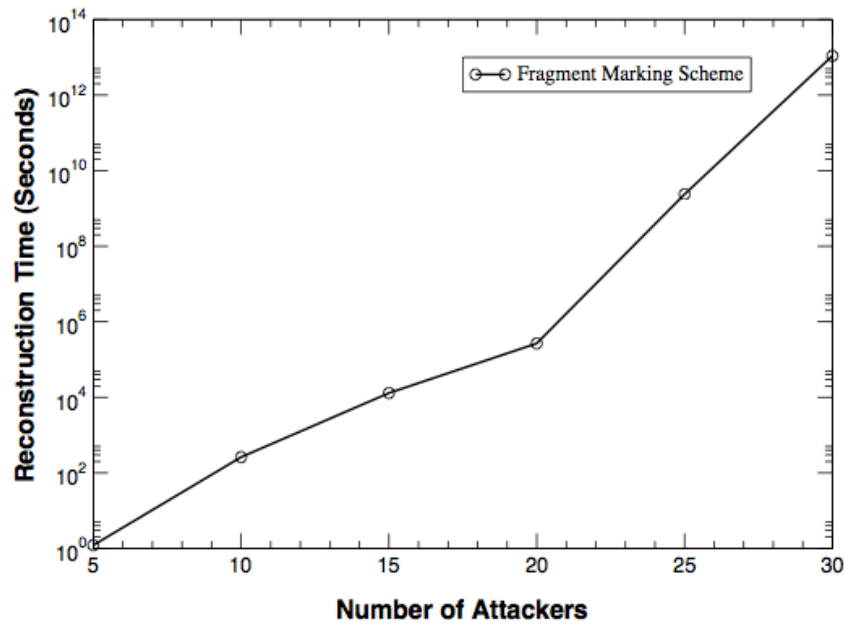


Fig. 11. Computation Overhead for FMS

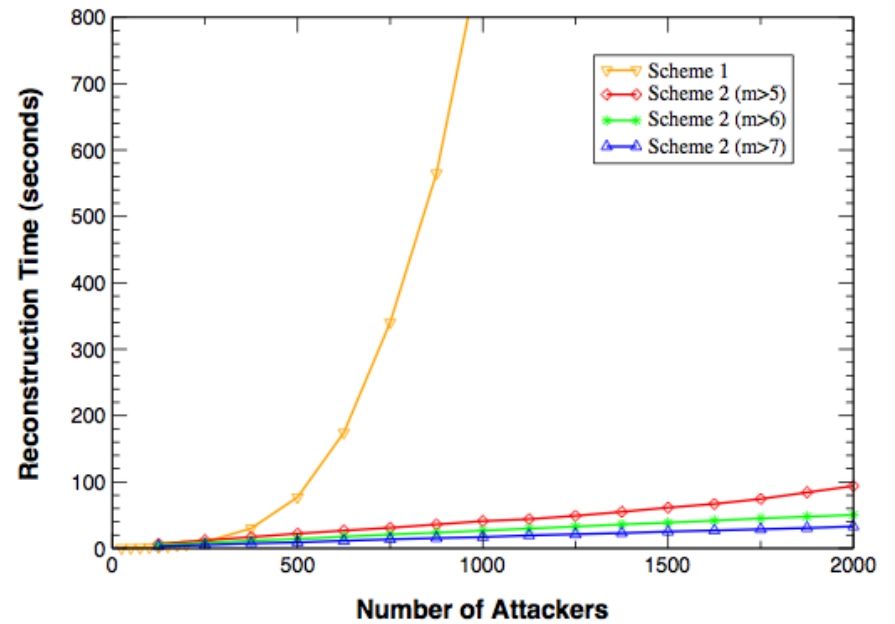


Fig. 9. Computation Overhead for Advanced Marking Schemes

Simulation Results: Number of packets required for reconstruction

One attacker

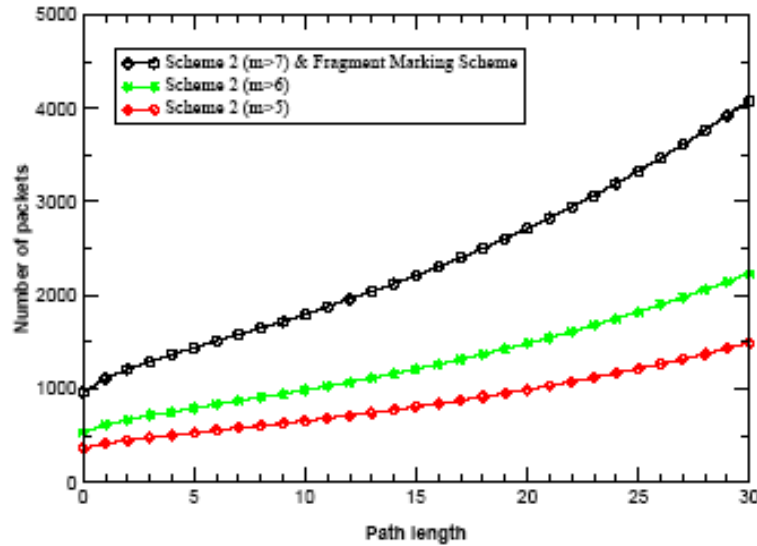


Fig. 12. Number of Packets Required for Reconstruction ($q = 4\%$)

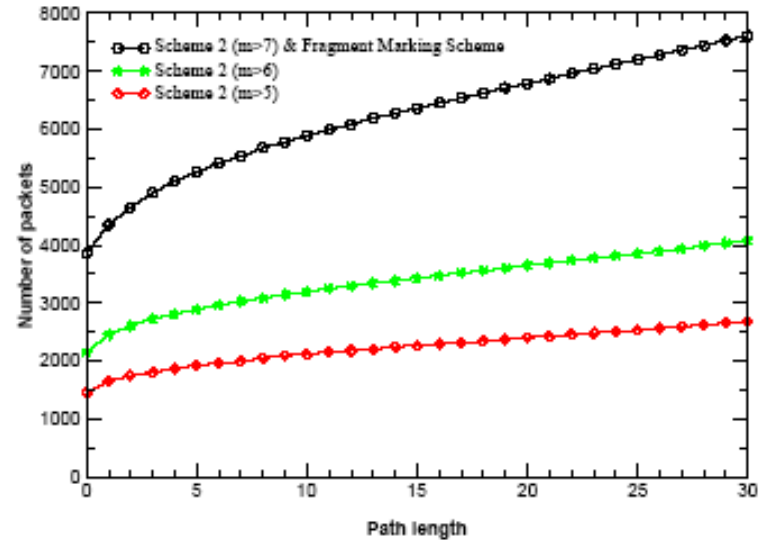


Fig. 13. Number of Packets Required for Reconstruction ($q = 1\%$)

Authenticated Marking Scheme

- Shortcoming of advanced techniques is that markings are not authenticated – thus markings can be forged.
- One solution is to use RSA digital signatures – expensive!

Authenticated Marking Scheme

- Authentication with a MAC
 - MAC : message authentication codes
 - Two parties can share a secret key K , for example, a router R_i shares a unique secret key K_i with the victim.
 - Instead of hash function, the IP address and packet specific information is encoded with a MAC function using the key.
 - Disadvantage : share a secret key with each potential victim – **Impractical!**

Authenticated Marking Scheme

- Time-Released Key Chains
 - Basic idea
 - Each router R_i first generates a sequence of secret keys, $\{K_{j,i}\}$ (where each key $K_{j,i}$ is an element of a hash chain) by successively applying a one-way function g .
 - Because g is a one-way function, anybody can compute forward(backward in time) but not backward (forward in time).
 - After router R_i uses $K_{t,i}$ as the key to compute the MAC, it reveals the key $K_{t,i}$ after a delay of σ

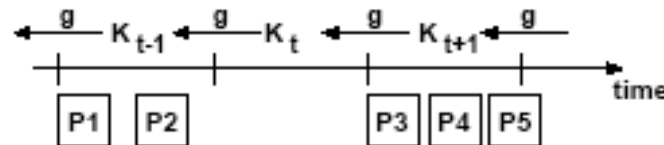


Fig. 14. Authenticated Marking Using a Time-Released Key Chain at a Router.

Follow-on Work

(1) Single-packet IP Traceback

IEEE/ACM Transactions on Networking, 2002

- Issue with previous techniques?

Require a number of packets to trace the attack path

- What about attacks having single packets!
- Idea: Use packet digest logs.

Follow-on Work

(2) Efficient Packet Marking for Large-Scale IP Traceback *ACM CCS, 2002*

- Goal : Improve practicality and security of PPM.
- Improvement of “Advanced and Authenticated techniques” paper.
- Does not require the victim to know the “map”.
- Also does not require the packets to be signed individually.

(3) B. Al-Duwairi and G. Manimaran, “Novel hybrid schemes employing packet marking and logging for IP traceback,” *IEEE Transactions on Parallel and Distributed Systems, 2006.*

- Goal : Reduce the number of packets required in constructing the attack path by making use of packet logging.
- Idea: Preserve the mark if already contained in the packet by logging.

Follow-on Work

- (4) Chao Gong; Sarac, K, “A More Practical Approach for Single-Packet IP Traceback using Packet Logging and Marking,” *IEEE Transactions on Parallel and Distributed Systems*, 2008.
- Goal: Improve practicality of single packet IP traceback.
 - What does it improve? Storage overhead and access time.
 - **How:** Intelligent use of packet marking to help improve the scalability of log based IP traceback.
 - Partially record path info in packets, partially at routers.
- (5) *Coloring the Internet: IP Traceback*
IEEE Int Conference on Parallel and Distributed Systems, 2006
- Goal : Reduce the number of packets as well as number of marked bits per packet.
 - Use reusable colors as labels for routers.
 - Star graph coloring algorithm to trace attack path.

Follow-on Work

(6) TTL Based Packet Marking for IP Traceback

Globecom 2008

- Goal: Reduce false positives/ forged markings.
- Motivation : 50% of the packets are unmarked.
- Packet marked with probability inversely proportional to the distance it has to travel. (TTL value)

(7) Passive IP Traceback: Capturing the Origin of Anonymous Traffic through Network Telescopes

SIGCOMM 2010

- Goal : To design a technique that does not require ISP deployment, router deployment.
- Analyze the ICMP messages that are received by a network telescope as a result of spoofed messages travelling on internet.
- Internet route model is then used to reconstruct the attack path.