Towards an Analysis of Onion Routing

P. Syverson, G. Tsudik, M. Reed, C. Landwehr

cs6461
Computer Science, MTU
Byung Choi

Introduction

- Primary goal of onion routing: strongly private communication in real time over a public network at reasonable cost and efficiency
- NRL implementation supports 1.5 M connections per month as of 2000
- Second generation under way
-

Onion Routing Usage

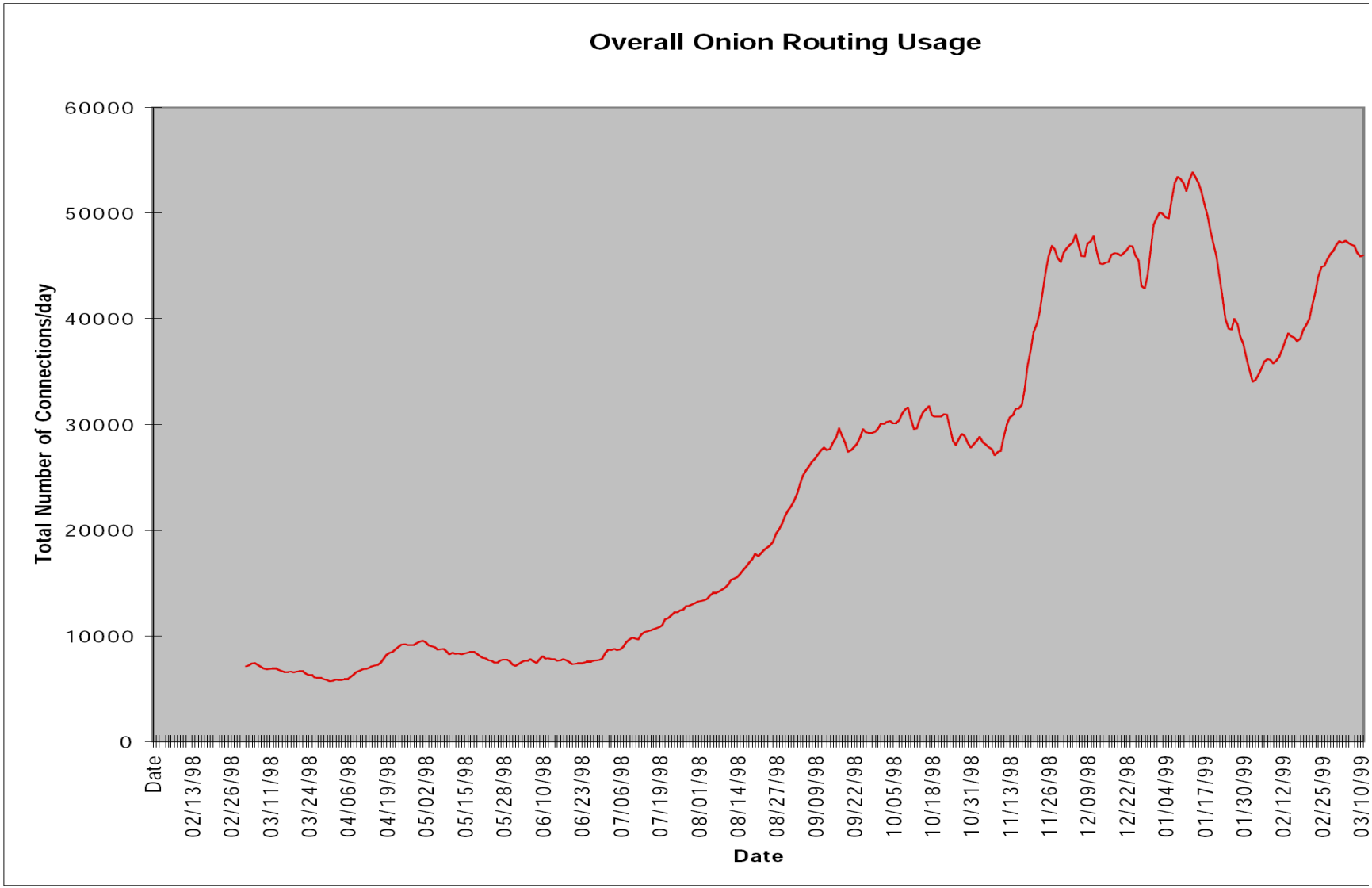

Figure 1: 30 Day Rolling Average of Onion Routing Usage: 3/1/98 – 3/1/99

Onion routing overview

- COR: Core Onion Router designed to pass information in real time, limiting mixing.
- Proxy-aware applications
  - HTTP, FTP, SMTP, ...
- Proxy
  - Application specific privacy filter
  - Application specific translator
  - Onion management layer
  - Proxy must know the topology and entry and exit policies!

Overview

- Longstanding TCP connections, thick pipes, anonymous connections, clique!
- Stream ciphers at each onion router
- 128 bytes cell
- Cell changes its appearance but not size, from input to putput
- Email, Web transactions, short lived, attack resistant
- Long lived? - FTP, SSH, ... attack susceptible

Security goals

- Sender activity
- Receiver activity
- Sender content
- Receiver content
- Source destination linking

Network model

- The network of onion routers is a clique, fully connected
- Bandwidth limited to a constant rate
- Exit policy at each node unrestricted
- For each route, each hop is chosen randomly
- The number of nodes in a route 2 – infinitive with r onion routers
  - Remote-COR configuration
  - Local-COR configuration

Network model

- Entrance policy via remote-COR unrestricted
- Entrance policy via local-COR is to exclude all but internal connections

Adversary model

- Observer
- Disrupter
- Hostile user
- Compromised COR
  - Single adversary
  - Multiple adversary
  - Roving adversary
  - Global adversary

Security assessment

- Roving adversary
  - Round?
  - Automatic healing?
  -