SWINBURNE UNIVERSITY OF TECHNOLOGY

An Empirical Evaluation of IP Time To Live Covert Channels

Sebastian Zander, Grenville Armitage, Philip Branch

{szander,garmitage,pbranch}@swin.edu.au

http://caia.swin.edu.au/cv/pbranch

Overview

- Covert channels and their applications
- Covert channels evaluation framework
- IP Time To Live (TTL) covert channel
- Future work

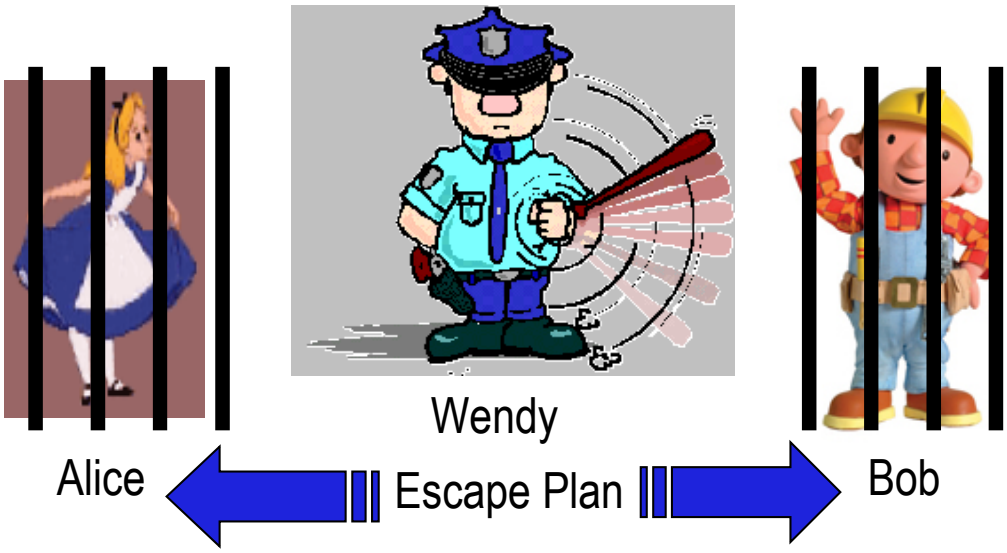
Covert Channels

- Encryption protects communication **only from being read** by third parties
- Covert channels **aim to hide the existence** of communication (stealth over capacity)
- Often covert channels use means of communication not intended for communication
- Huge amount of overt network traffic makes Internet ideal for 'high-capacity' covert communication

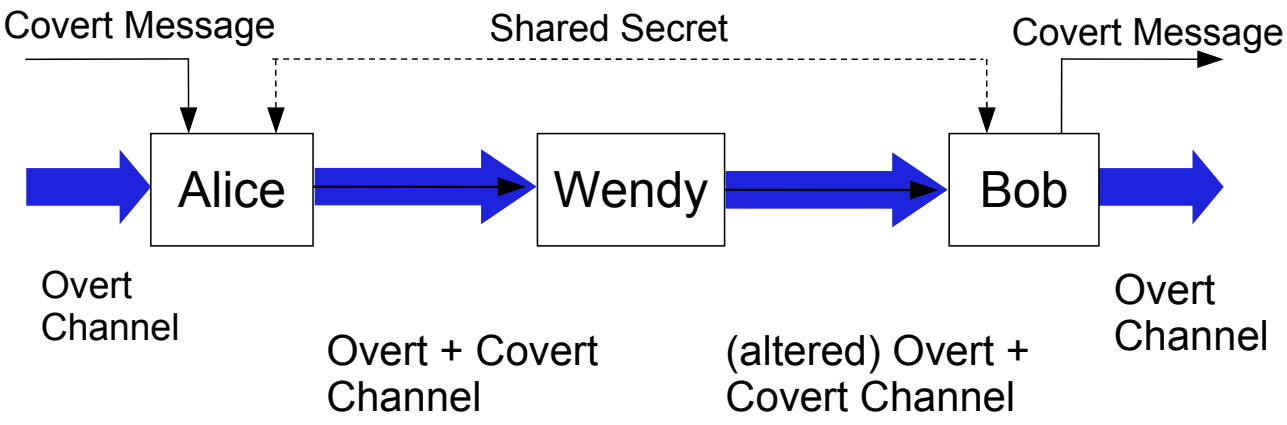
Covert Channel Applications

- Government agencies vs. criminals and terrorists hiding communication and coordination
- Hackers ex-filtrating data or controlling systems vs. system administrators hiding management traffic
- Ordinary users circumventing censorship or encryption laws (or just bypassing firewalls)
- Distribution and control of viruses, worms, bots

Covert Channel Model

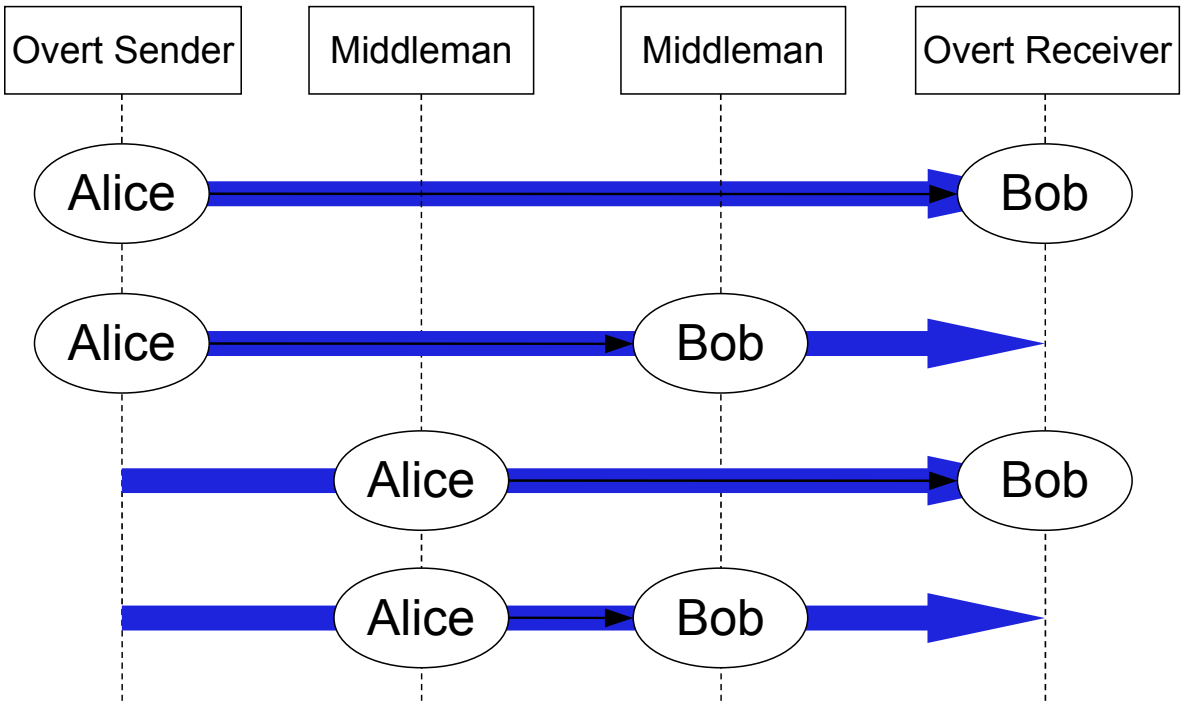


Covert Channel Model cont'd



- Only one direction shown (Alice sending to Bob)
- Wendy can be passive or active

Communication Scenarios

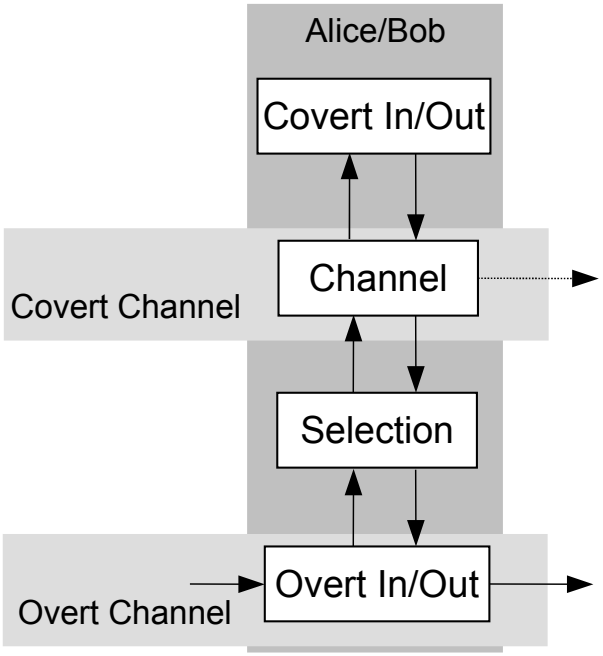


Software Evaluation Framework

- Covert Channels Evaluation Framework (CCHEF)
- Extensible to allow adding new covert channels without need to change framework
- Flexible to enable evaluation of covert channel characteristics across range of typical network conditions
  - Stealth/Security
  - Capacity
  - Robustness

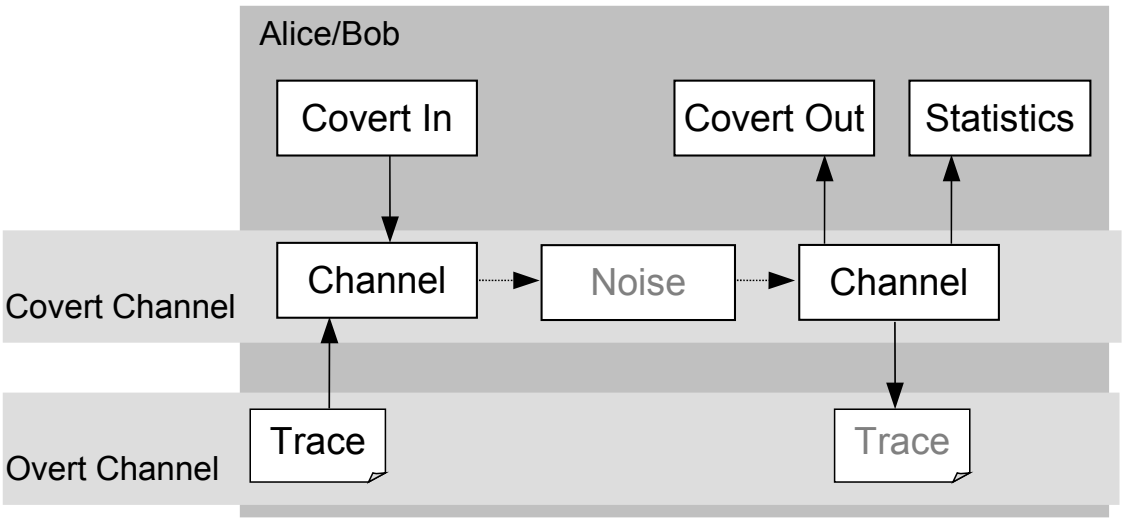
CCHEF Building Blocks

- Covert In/Out
  - Input/output of covert data
- Channel
  - Modulation, framing, error correction, encryption
- Overt packet selection
- Overt In/Out
  - Intercept/read packets, re-inject modified packets



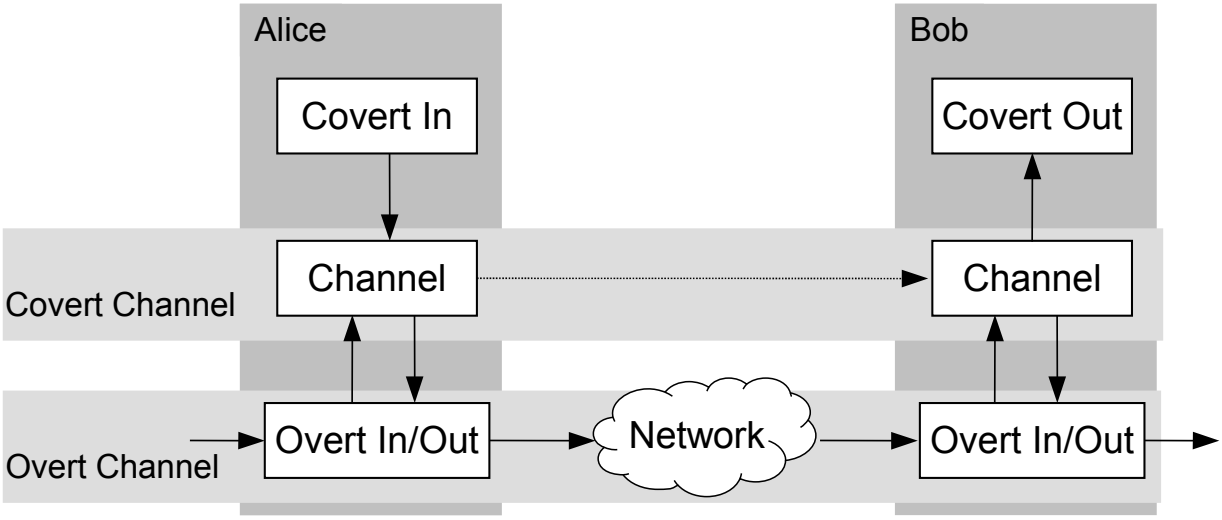
CCHEF With Emulated Overt Traffic

- Use overt traffic from trace (and add artificial noise)
- Alice and Bob are the same entity



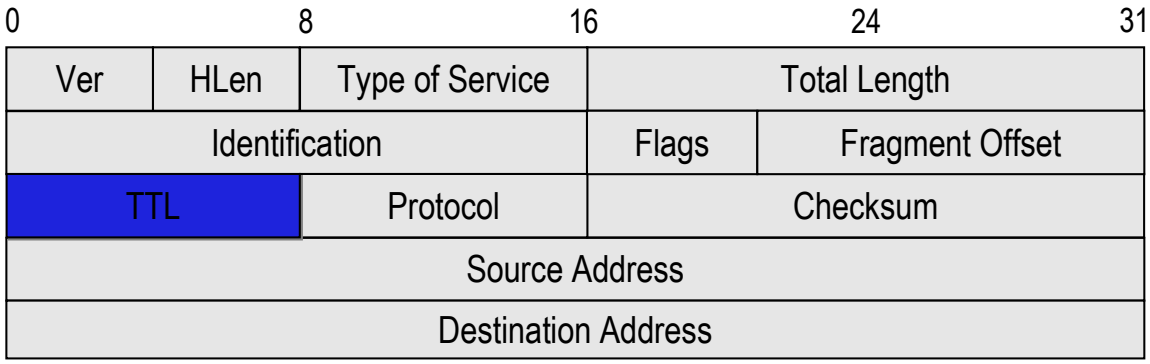
CCHEF Across Real Network

- Use real overt traffic across real network
- Alice and Bob are on two different hosts



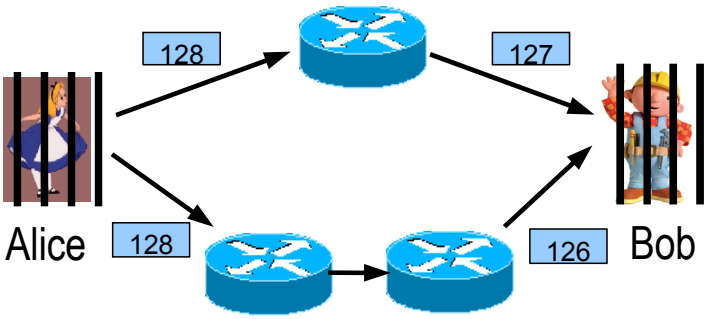
IP Time To Live (TTL)

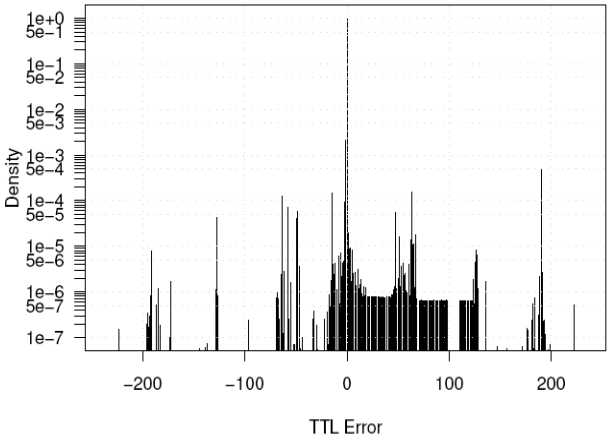
- TTL limits lifetime of IP packet in network
- Sender sets initial TTL value
- Each router decrements TTL value
- Packet with TTL=0 is discarded



Channel Noise

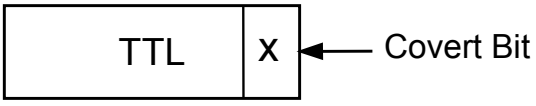
- TTL is modified by routers and packets take different paths from sender to receiver
- Also middleboxes (e.g. firewalls) change TTL



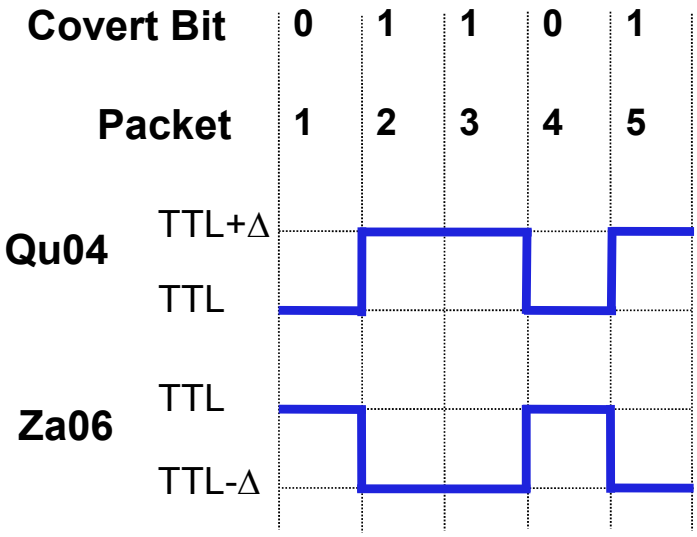


Channel Encodings

- Encode covert bit directly into TTL (Qu04-1, Scheme1)

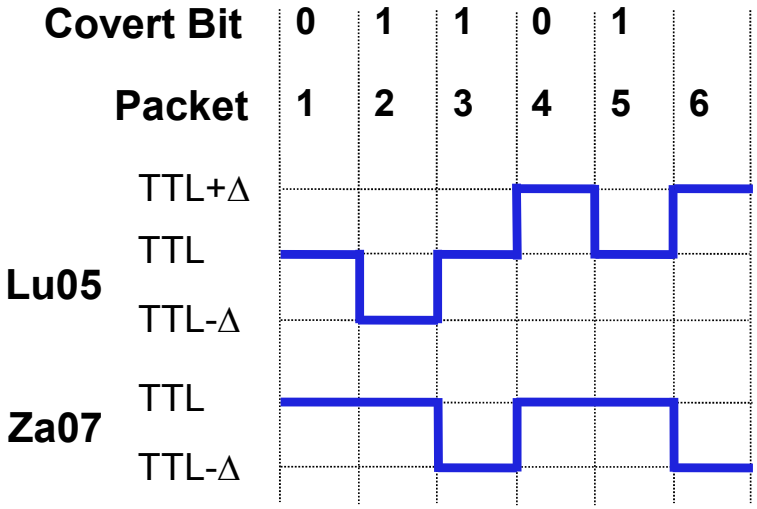


- Map covert bit to different TTL values (Qu04-2, Zander06)



Channel Encoding cont'd

- Encode covert bits as difference of TTL values of consecutive packets (Lucena05, Scheme2)

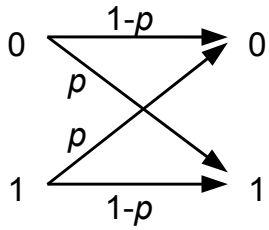


Benefits of New Encoding Schemes

- Only decrease initial TTL
  - Prevent immortal packets (chances depending on Δ)
  - Use overt traffic with high initial TTL (e.g. 255)
  - Avoid suspicious TTL values if warden at next hop (e.g. TTL values of 65 or 129)
- Limit number of TTL values used (Scheme2)
  - Lu05 potentially uses whole number space

Channel Capacity

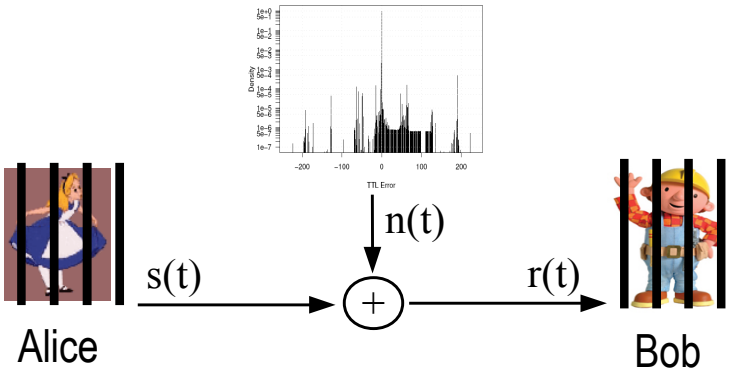
- Binary (A)Symmetric Channel (BSC/BAC)



- Compute capacity based on error probability

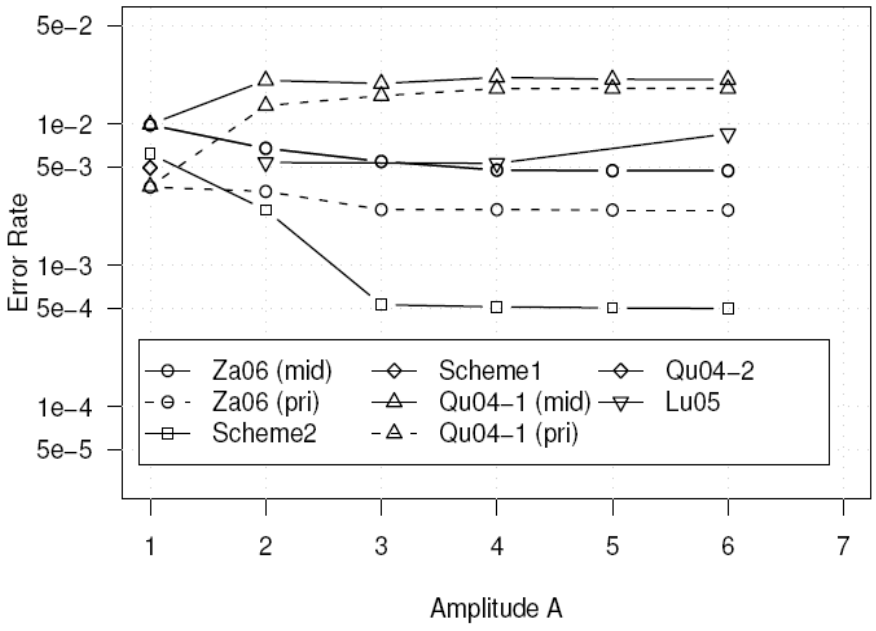
$$C = 1 + p \cdot log_2(p) + (1-p) \cdot log_2(1-p)$$

- Estimate error probability from traffic traces



Error Rates

- 5 packet traces
- Unif. random covert data
- 8 encoding schemes
- Different amplitudes (Δ)
- 5 runs each



Result for Leipzig-II (others in paper)

Transmission Rates

- Transmission rate in bits/second: $R = C(p)/f$ where $C(p)$ is the capacity and f the overt packet frequency

Dataset	Direct	Qu04-1 pri | mid	Za06 pri | mid	Lu05	Scheme2
Twente	481	483 | 437	483 | 437	439	444
Waikato	1396	1398 | 1095	1426 | 1104	1197	1206
Bell	173	212 | 203	229 | 213	208	207
NZIX	2037	2378 | 1935	2390 | 1961	2259	1515
Leipzig	11.6k	10.7k | 10.2k	11.7k | 10.2k	10.5k	10.5k

Summary & Future Work

- Implemented covert channels evaluation framework (http://caia.swin.edu.au/cv/szander/cc/cchef/)
- Covert channel in TTL field
  - Proposed two new encoding schemes
  - Examined channel noise and proposed channel model
  - Evaluated channel capacity
- Future Work
  - Include overt packet loss and reordering
  - Develop methods for detection and elimination

The End

Questions?

SWINBURNE UNIVERSITY OF TECHNOLOGY