SWINBURNE UNIVERSITY OF TECHNOLOGY

Error Probability Analysis 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/szander

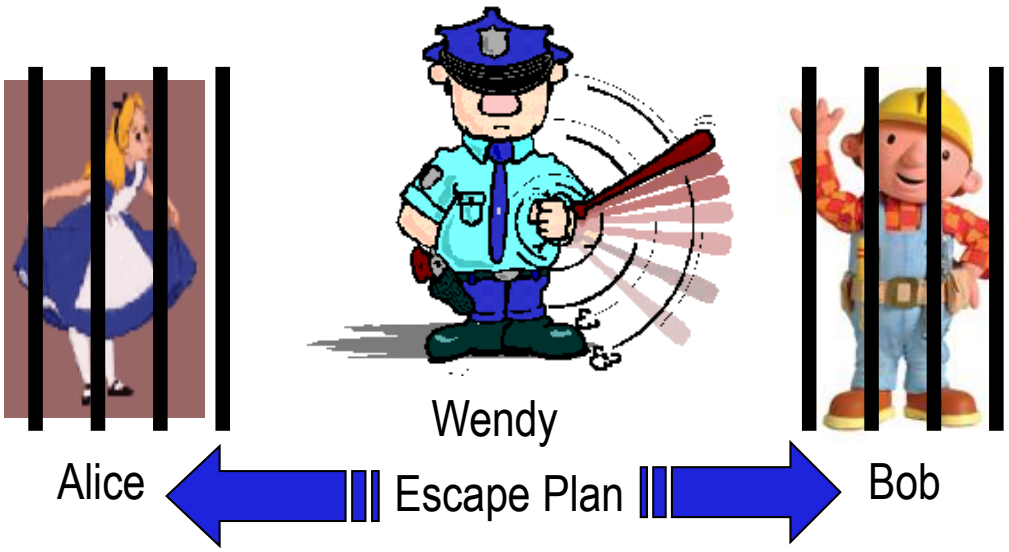
Covert Channels

- 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 (hidden inside overt traffic)

Covert Channel Applications

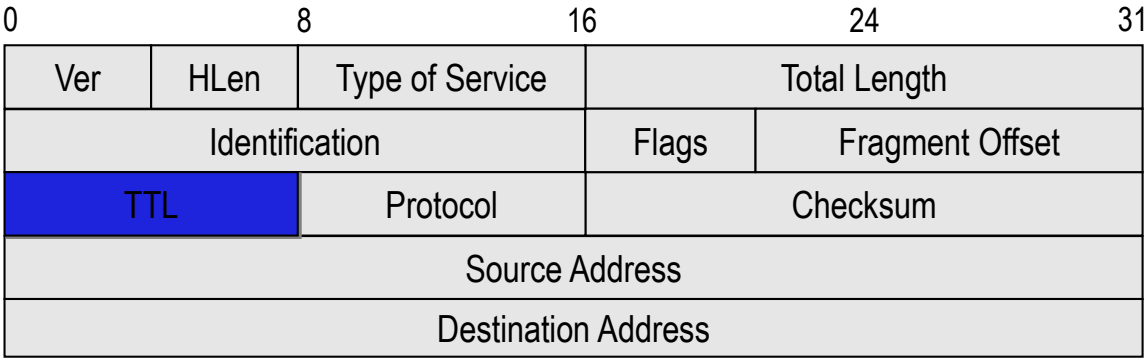
- Government agencies vs. criminals and terrorists hiding communication and coordination
- Hackers ex-filtrating data or controlling systems vs. system administrators hiding management traffic
- Ordinary users circumventing censorship or strong encryption laws (or just bypassing firewalls)
- Distribution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

Covert Channel Model



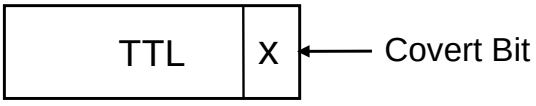
IP Time To Live (TTL)

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

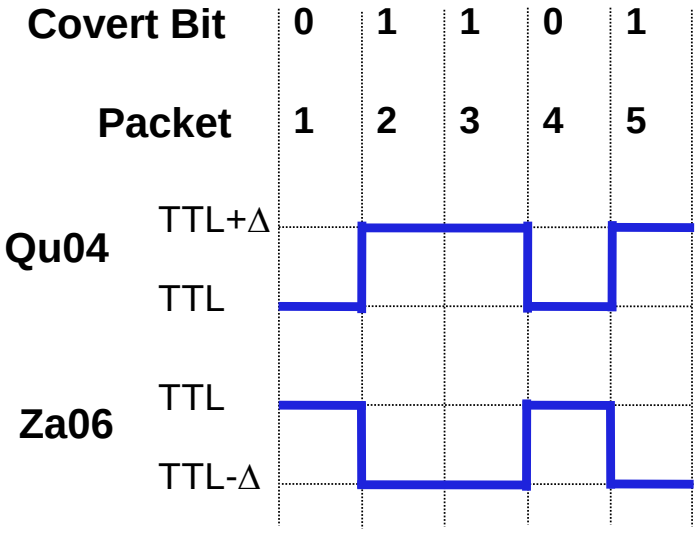


Covert Channel Encoding

- Encode covert bit into TTL LSB (Qu '04)

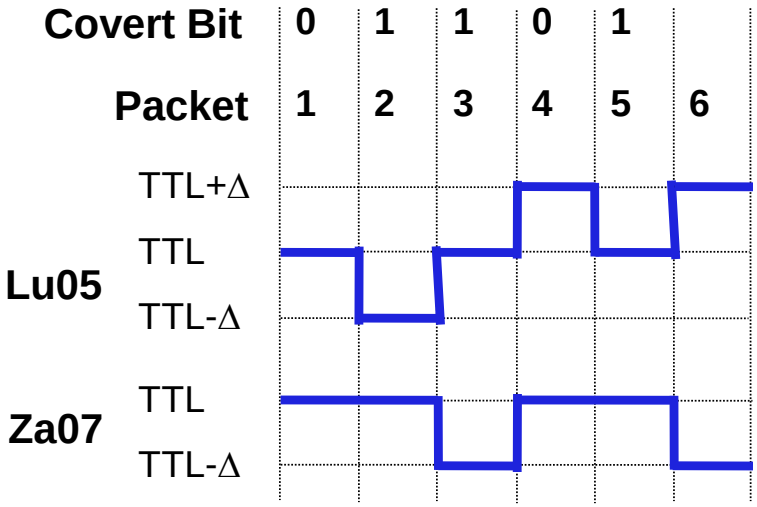


- Encode covert bits as different TTL values (Qu '04, Zander '06)



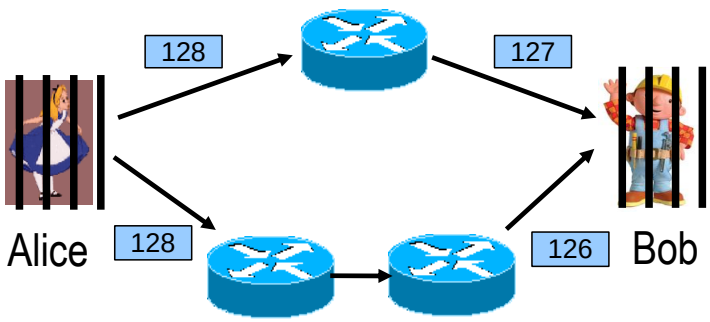
Covert Channel Encoding

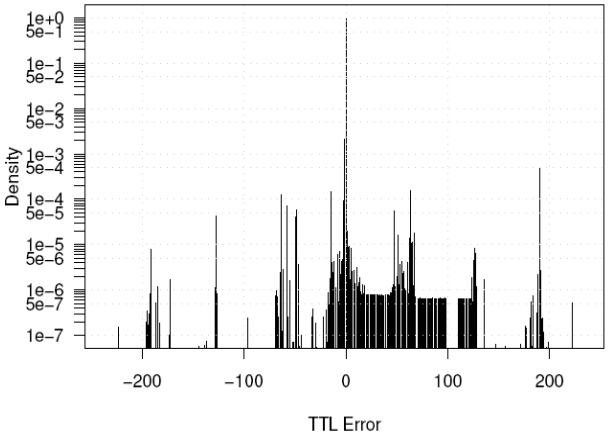
- Encode covert bits as TTL change between two packets (Lucena '05 and Zander '07)



Covert Channel Noise

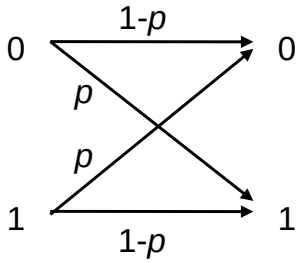
- TTL is modified by routers and packets take different paths from sender to receiver
- Also middleboxes (e.g. firewalls) change TTL





Covert Channel Capacity

- Model TTL channel as Binary (A)Symmetric Channel (BSC/BAC)
- Capacity can be computed based on error probability
- Error probabilities derived (see paper)

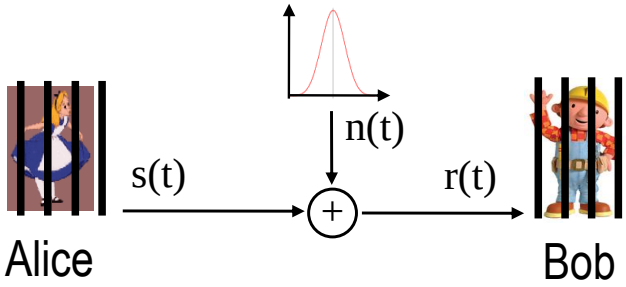


$$C = 1 + p \cdot log_2(p) + (1-p) \cdot log_2(1-p)$$

$$p = \sum_{k=-128}^{127} P(X = 2k+1)$$

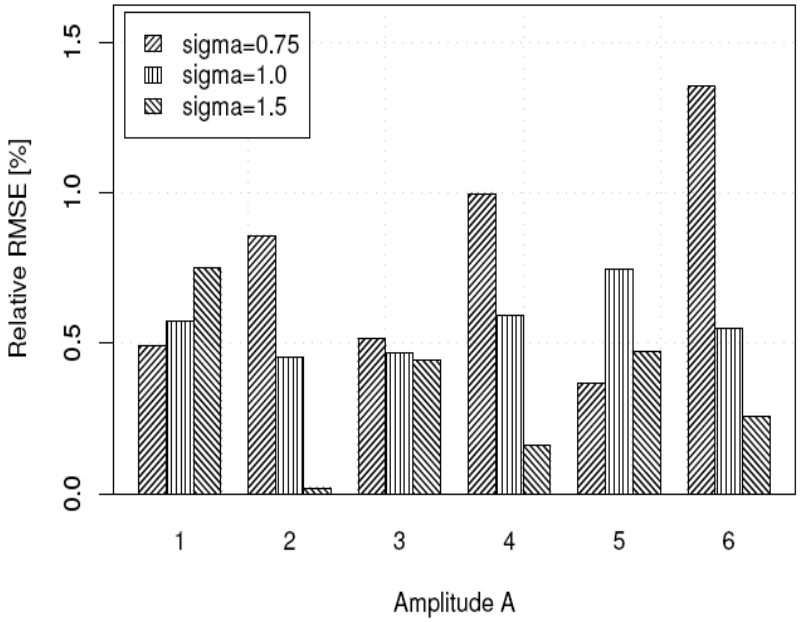
Simulation Environment

- Developed framework for simulating network protocol covert channels
- Implemented different TLL covert channel encoding schemes
- Compare analytical error probabilities with simulation (modelled TTL variation as additive Gaussian noise)



Error between Simulation and Analysis

- 42 million packets
- Different std. dev. of noise (σ)
- Different amplitudes (Δ)
- 20 runs each
- Relative Root Mean Squared Error (RMSE)



Result for Za06 (others in paper)

Conclusions & Future Work

- Derived error probabilities for different TTL covert channel encodings
- Developed covert channel simulation environment (http://caia.swin.edu.au/cv/szander/cc/cchef/)
- Analytical error probabilities and simulation results are good match
- Future: extend channel model & simulation environment
  - ☐ Include overt packet loss and reordering
  - ☐ Use real TTL error based on packet traces (emulation)

The End

Questions?