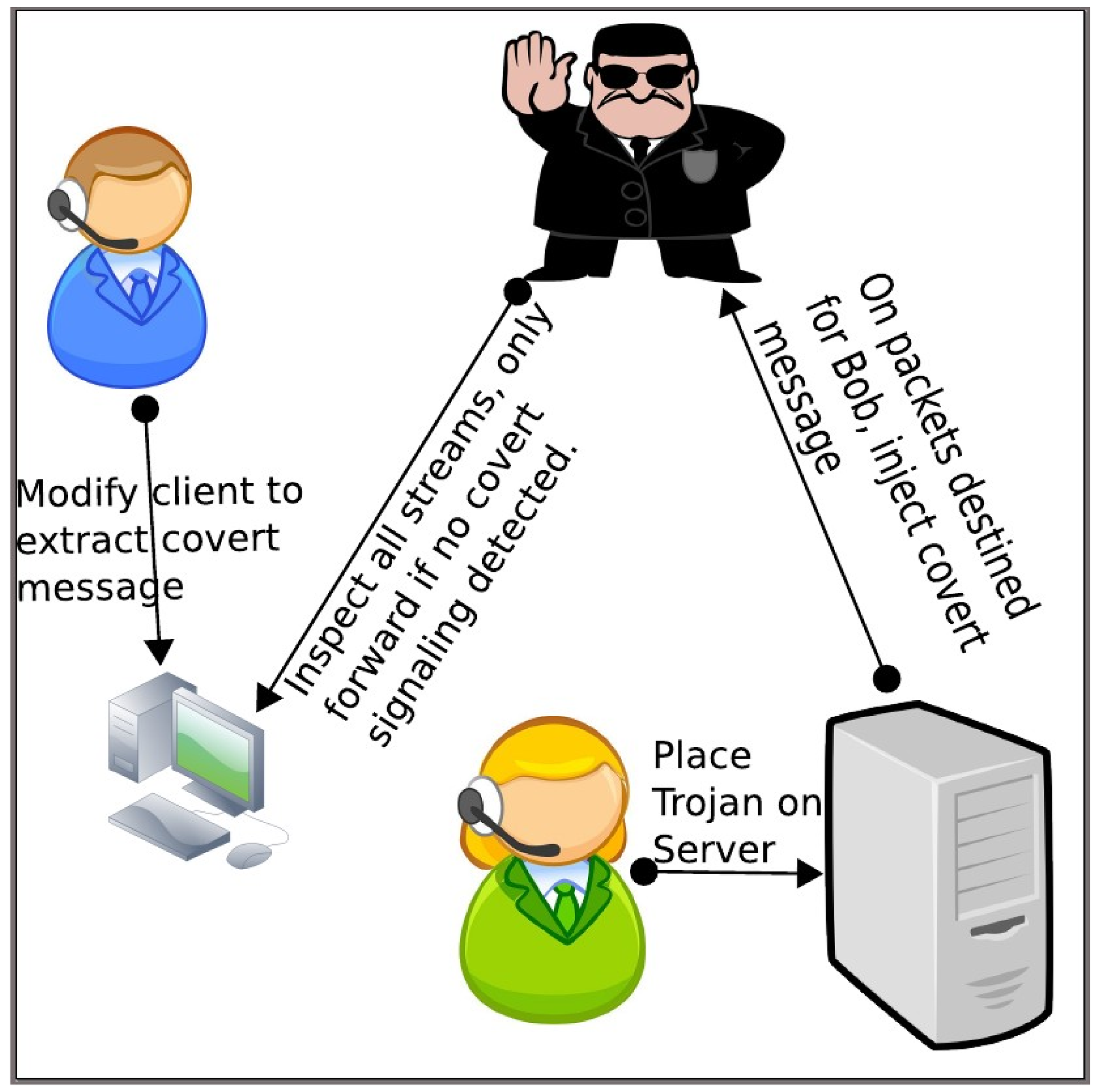
Enhancing Covert Communications with Multiple Colluding Receivers

Michael Clark and Sneha Kumar Kasera
School of Computing, University of Utah
{mikec, kasera}@cs.utah.edu

Introduction



Traditional (single receiver) system setup:
- Choose exploit field (e.g. last byte of TCP Timestamp)
- Alice: probabilistically inject parts of coded message into field
- Bob: extract symbols from field, decode to correct errors
- Warden: assume full knowledge of system and keys

Can we create undetectable system?

Previous detection work:
- Signatures – published exploits thwart easily
- Anomaly – qualitative arguments until statistical methods in [1]
- Brute-Force – never mentioned in literature, significant oversight

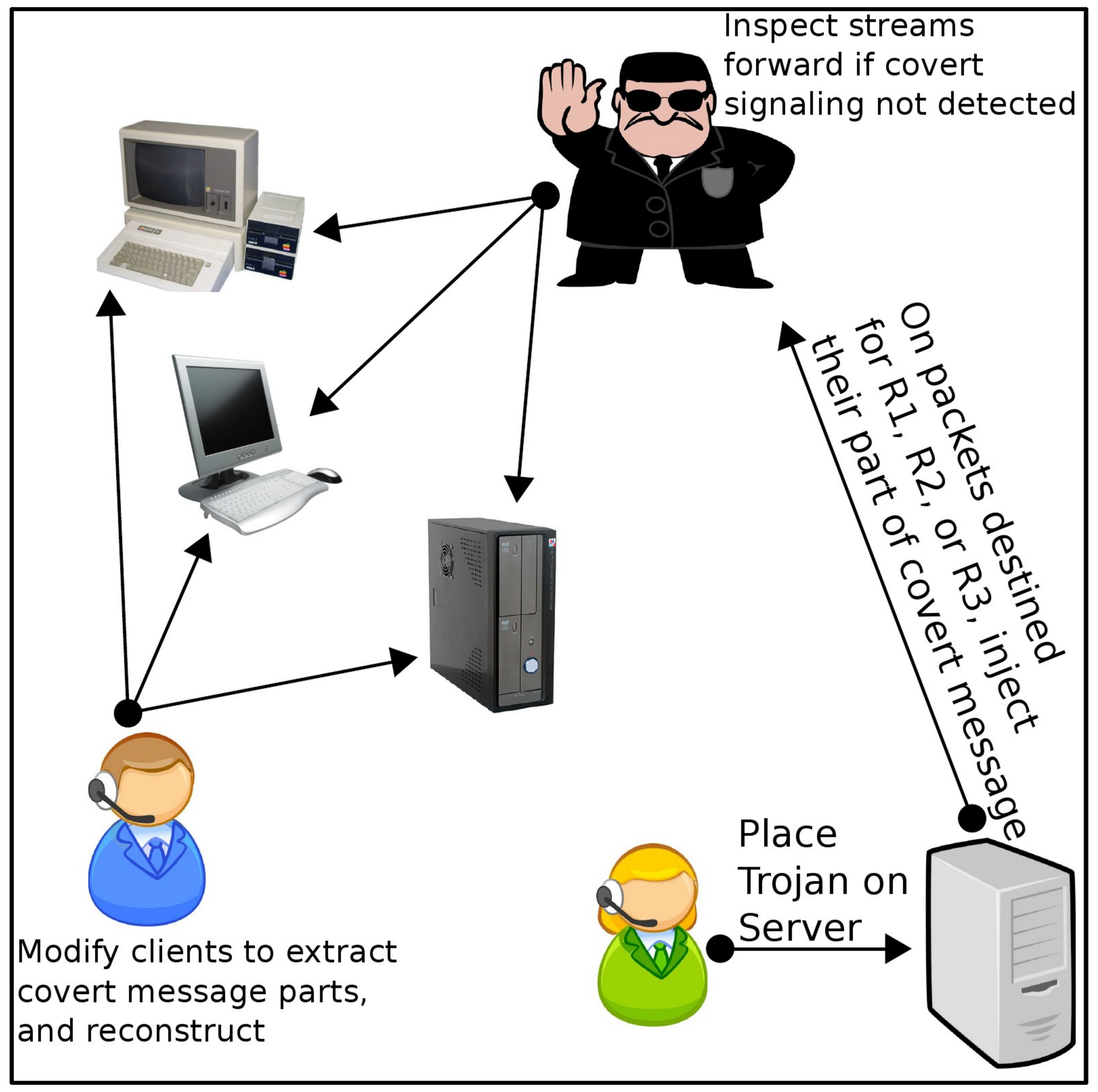
Contributions

Thwarting Brute-Force Detection:
- Propose multiple colluding receiver design
- Verify possibility of brute-force in single receiver system
- Show our design's resilience to threat

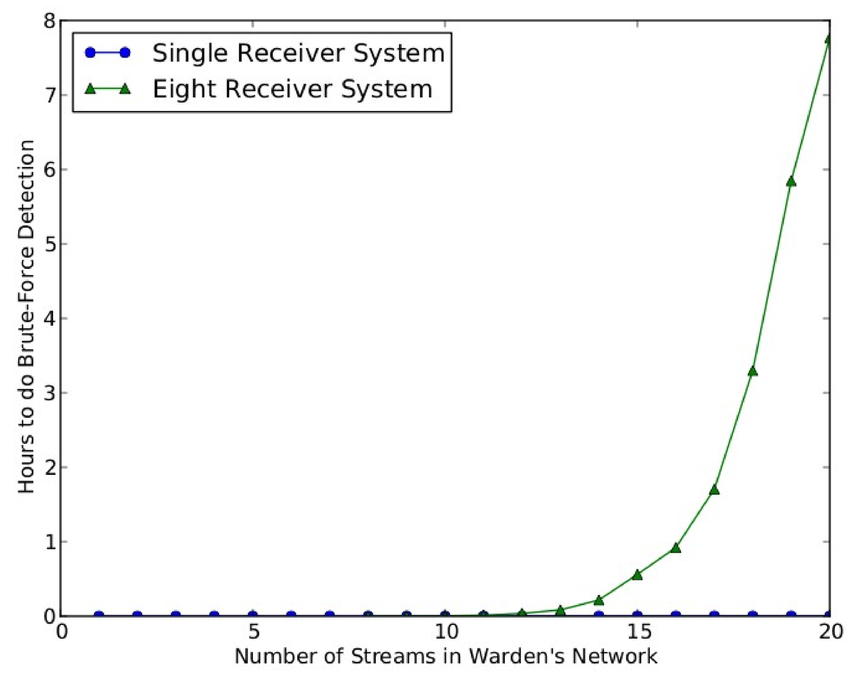
Thwarting Anomaly Detection:
- Propose better quantification technique
- Provide fast approximation

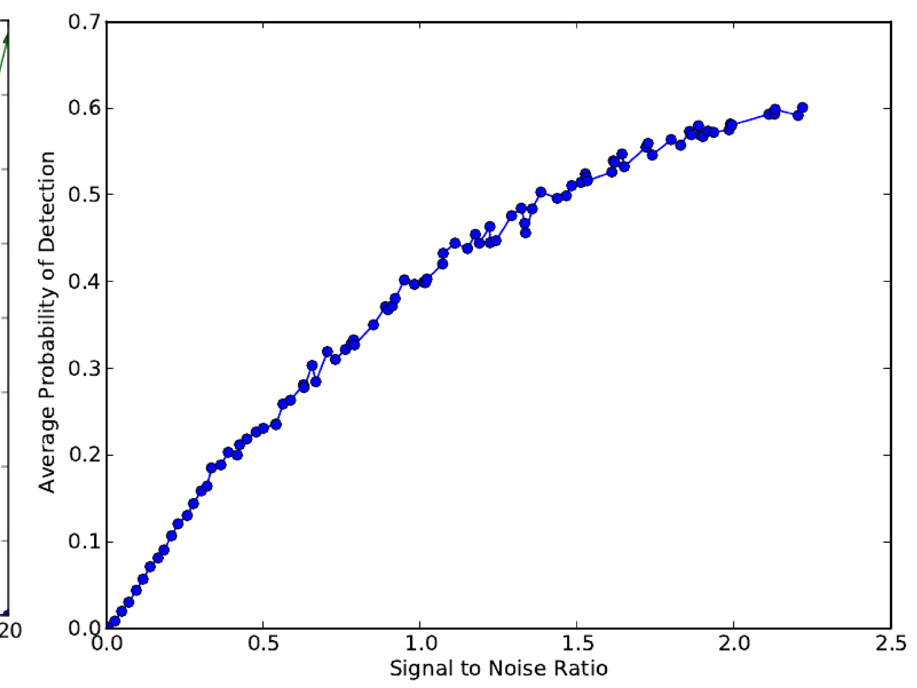
Multiple Receiver Design

Multiple receiver system setup:
- Split coded message, inject parts to each receiver
- Decoding depends on all receivers
- Receivers extract symbols, share them to decode



Brute-Force Detection:
- Single receiver, for each stream in network decode exploit field
- Multiple receivers, decode all combinations of r streams





Detection Quantification

Goal: Conservative estimate for probability of detection
- $S \leftarrow$ sequence of symbols from exploit field w/o injection
- Injection process = f: $S \rightarrow S'$
- For symbol s use diff. between S and S' to calc. probability

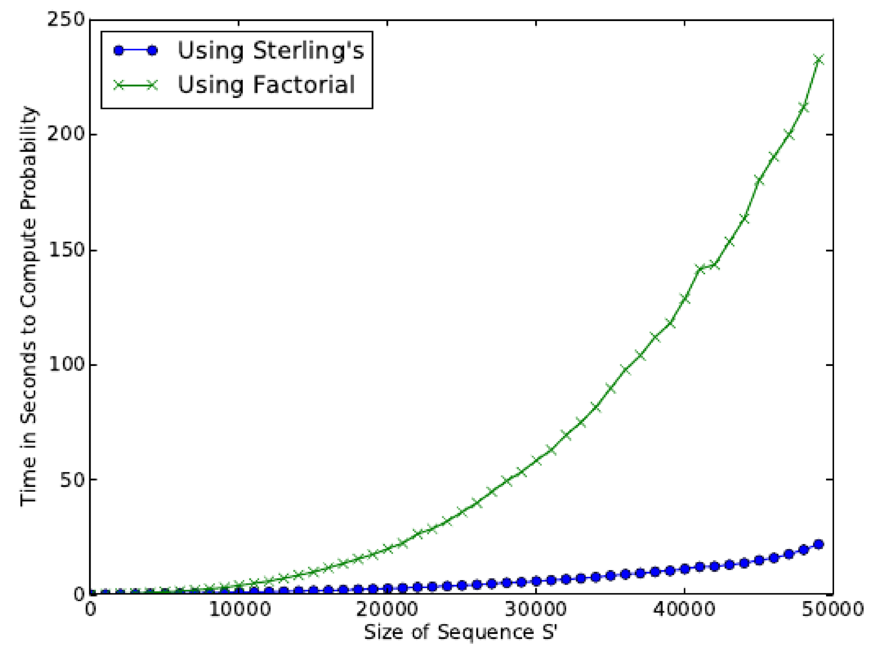
$$p_{anom}(s) = 1 - \sum_{x=0}^{UCL(s)} \binom{|S'|}{x} (\rho_{S'}(s))^x (1-\rho_{S'}(s))^{|S'|-x}$$

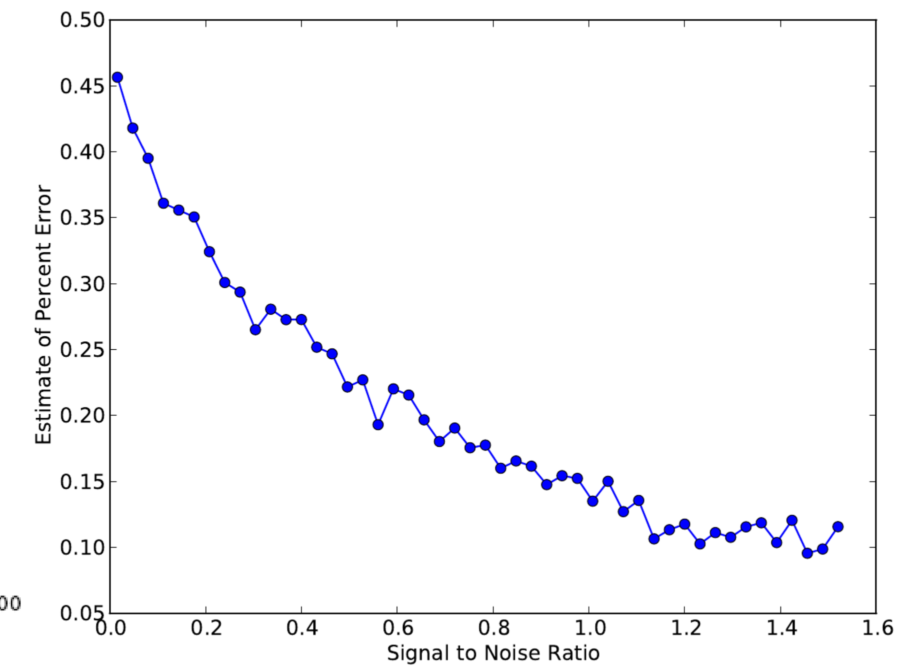
- ***UCL(s)*** **-** comes straight from statistical quality control [2]
- **ρ -** calculates the rate of occurrence of s in sequence

Use estimate for single symbol, quantify detection
- Let U be the alphabet of covert message
- Quantify detection of each s in U then combine

$$p_{sysDetect}(s) = 1 - \prod_{s \in U} (1 - p_{anom}(s))$$

Approximation Method:
- Calculating binomial coefficient is slow if $|S'|$ is large
- Use Sterling's Approximation for factorial [3]

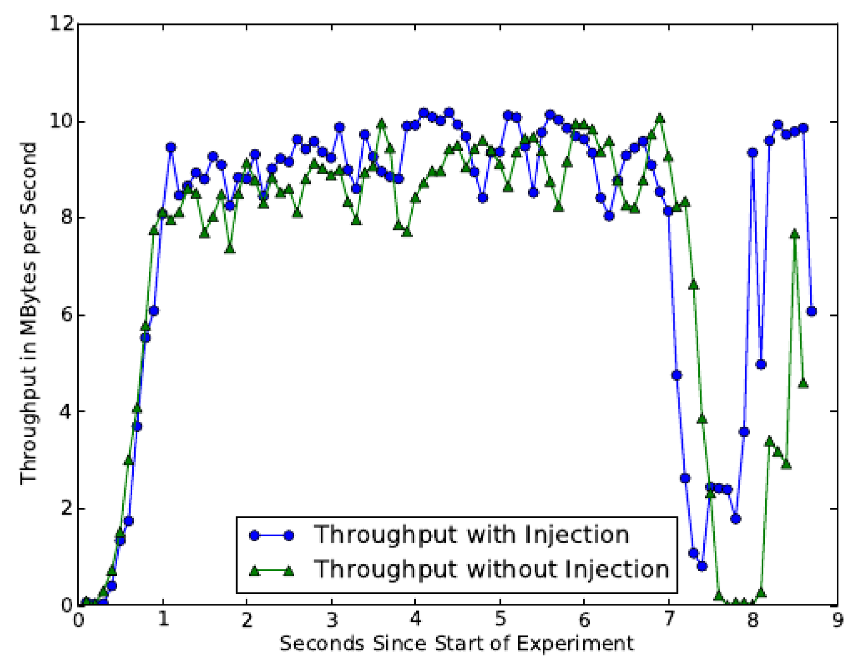


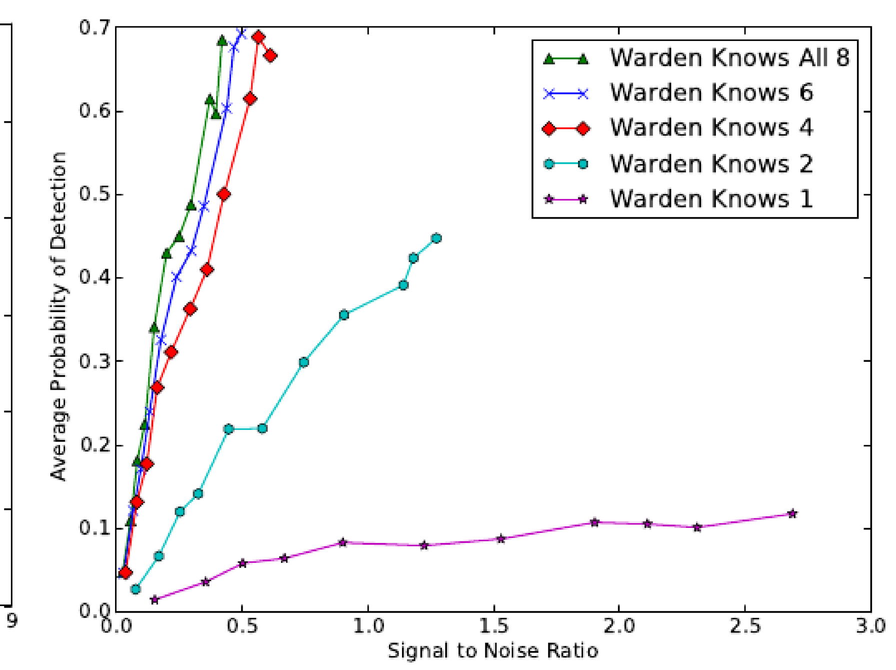


Implementation

CovertSSH, a trojaned version of OpenSSH-5.3p1
- SSH uses Binary Packet Protocol (BPP) for transportation
- Use last byte of BPP's random padding field for exploit

Using Emulab [4] we experiment with our system
- Inject headlines from USA Today newspaper





Future Work

- Steganography, anonymity, watermarking
- Deniability

References

[1] Ronald William Smith and George Scott Knight. *Predictable design of network-based covert communication systems.* IEEE Security & Privacy 2008.
[2] Eugene L. Grant and Richard S. Leavenworth. *Statistical Quality Control.* Mcgraw-Hill, 1996.
[3] David MacKay. *Information Theory, Inference, and Learning Algorithms.* Cambridge University Press, 2002.
[4] http://www.emulab.net