ON THE CHANNEL CAPACITY OF NETWORK FLOW WATERMARKING

Amir Houmansadr Siva Gorantla Todd Coleman Negar Kiyavash Nikita Borisov
University of Illinois at Urbana-Champaign

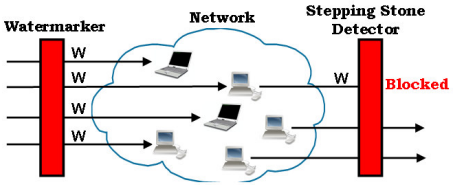
Network Flow Watermarking

Network flow watermarking is manipulating content independent patterns of network flows, e.g., packet timings, in order to perform traffic analysis.

Applications

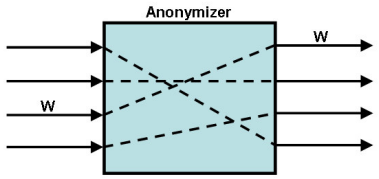
1- Stepping Stone Detection

Stepping stones are relays used by network intruders in order to conceal their identities.
• Flow watermarking can be used to detect relayed traffic.



2- Compromising Anonymity

Anonymous networks try to hide the relation between senders and receivers of network flows, e.g., TOR.
• Colluding attackers can use flow watermarking to break anonymity promises by linking senders/receivers.



Problem statement

Lack of information theoretical analysis of network flow watermarking in the literature

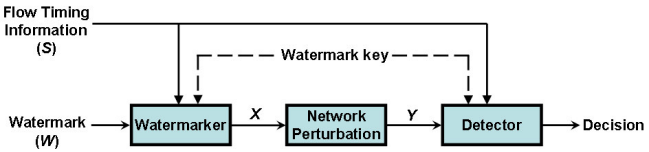
Challenge:

Non-memoryless behavior of timing channels

Flow watermarking types

1. Private watermarking: access to original flow at the detector
   • Focus of this research
2. Public watermarking: no access to original flow at the detector

Private watermarking model



• System modeling:
  • Flow timing information: side information *S*
  • Watermark sequence: message to be communicated
  • Computer network: a non-memoryless communication channel for timing information
  • Side information is shared between watermarker (encoder) and watermark detector (decoder)
  • Watermark key shared between sides

Capacity of memoryless channel

A. Asymptotic Equilibrium Property

• **Asymptotic Equipartition Property** (AEP) holds for a random process *X* if the empirical entropy is ε-close to its true entropy [2]:

$$-\frac{1}{n}\log p(X_1, X_2, \ldots, X_n) \xrightarrow{prob.} H(X)$$

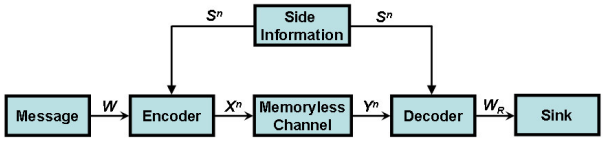
➢ Analog of the law of large numbers in information theory
• Theorem: AEP holds for i.i.d. processes
• The high probability region containing such sequences is called the **typical set.**

Joint AEP: holds for two random processes *X* and *Y* if the empirical marginal and joint entropies are ε-close to the true entropies [2].
• Theorem: Joint AEP holds for (X^n, Y^n) drawn i.i.d. according to

$$p(x^n, y^n) = \prod_i p(x_i, y_i)$$

B. Communication channel with shared side information

• This problem is equivalent to the private watermarking problem except for the channel
• Communication channel is memoryless



• The channel capacity is found to be [1]: $C=I(X;Y|S)$
• Proof methodology:
  • Generating a random codebook with rows and columns corresponding to messages and side info, respectively.
  • Encoder sends the appropriate cell content from the codebook
  • By receiving the altered message, Y^n, receiver looks for a cell from the codebook whose content is *jointly typical* with the received sequence. The index of this cell is returned as the message.

Non-memoryless approach

• We use the Exponential Server Timing channel (ESTC) to represent the flow watermarking channel.
➢ The system model is the same as 6.2 except for the channel which is non-memoryless → so, AEP does not hold generally.
❖ We intend to leverage the results of 6.2 by:
  ❖ using the observation of [3] that the ESTC channel is memoryless conditioned upon intermediate queue states
  ❖ show that AEP holds for some coding scheme

References

[1] J. Wolfowitz. Coding Theorems of Information Theory. Springer-Verlag, 3rd edition, 1978.
[2] T. M. Cover and J. Thomas. Elements of Information Theory. New York:Wisley, 2nd ed., 2006.
[3] T. P. Coleman, "A Simple Memoryless Proof of the Capacity of the Exponential Server Timing Channel," IEEE Information Theory Workshop, 2009.