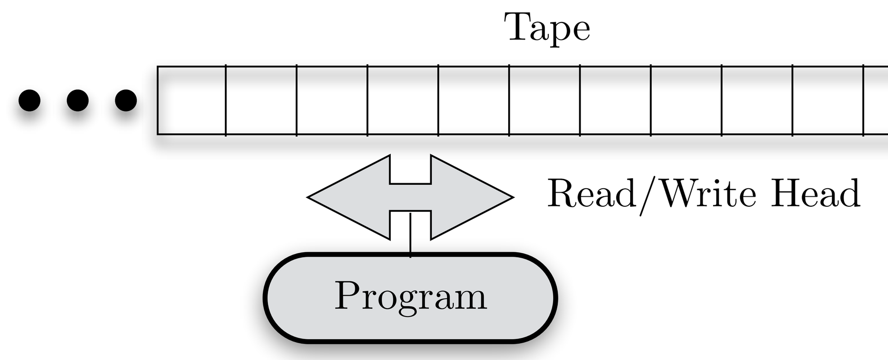
DETECTABILITY OF DENIAL-OF-SERVICE ATTACKS ON COMMUNICATION SYSTEMS

Holger Boche[1], Rafael F. Schaefer[2], H. Vincent Poor[3]
[1] Technische Universität München
[2] Technische Universität Berlin
[3] Princeton University

Turing Machine



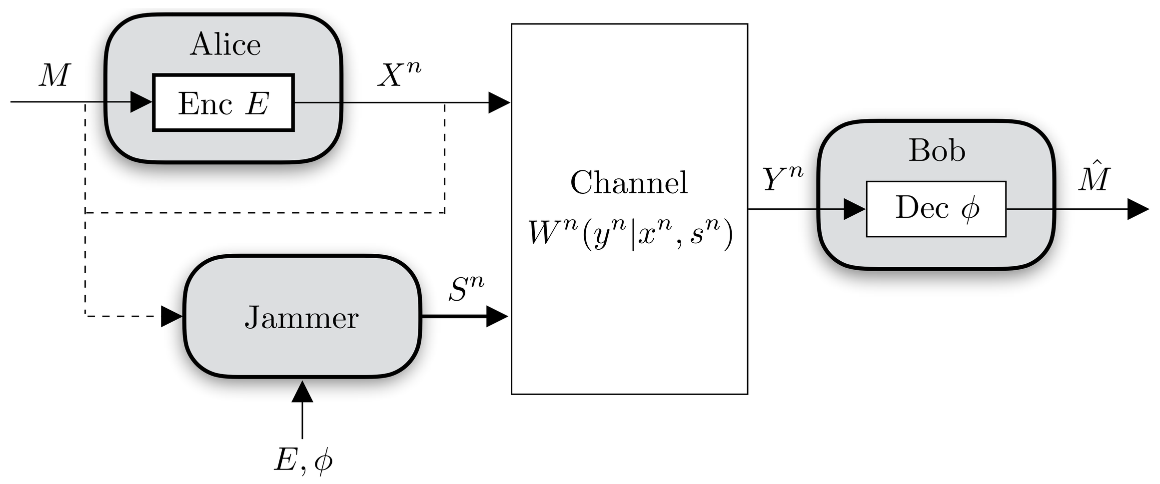
Mathematical model of an abstract machine that manipulates symbols on a strip of tape according to certain given rules

- Turing machines can simulate any given algorithm and therewith provide a simple but very powerful model of computation
- **No** limitations on computational complexity, unlimited computing capacity and storage, and execute programs completely error-free

$\Rightarrow$ **Fundamental performance limits for today's digital computers**

A. M. Turing, "On computable numbers, with an application to the Entscheidungsproblem," *Proc. London Math. Soc.*, vol. 2, no. 42, pp. 230–265, 1936

Communication System



- Let $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{S}$ be finite input, output, state (jamming) alphabets
- For fixed $s^n \in \mathcal{S}^n$, the DMC is $W^n(y^n|x^n, s^n) = \prod_{i=1}^n W(y_i|x_i, s_i)$

Definition: The *arbitrarily varying channel (AVC)* $\mathfrak{W}$ is given by

$$\mathfrak{W} = \{W(\cdot|\cdot, s)\}_{s\in\mathcal{S}}.$$

$$F(\mathfrak{W}) = \min_{U\in\mathcal{CH}(\mathcal{X};\mathcal{S})} \max_{x\neq\hat{x}} \sum_{y\in\mathcal{Y}} \Big| \sum_{s\in\mathcal{S}} W(y|\hat{x}, s)U(s|x) - \sum_{s\in\mathcal{S}} W(y|x, s)U(s|\hat{x}) \Big|$$

$\Rightarrow$ $\mathfrak{W}$ is *symmetrizable* if and only if $F(\mathfrak{W}) = 0$

Theorem: *The capacity $C(\mathfrak{W})$ of an AVC $\mathfrak{W}$ is*

$$C(\mathfrak{W}) = \begin{cases} \min_{q\in\mathcal{P}(\mathcal{S})} C(W_q) & \text{if } F(\mathfrak{W}) > 0 \\ 0 & \text{if } F(\mathfrak{W}) = 0 \end{cases}$$

with $W_q(y|x) = \sum_{s\in\mathcal{S}} W(y|x, s)q(s)$.

R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Z. Wahrscheinlichkeitstheorie verw. Gebiete*, vol. 44, no. 2, pp. 159–175, Jun. 1978

I. Csiszár and P. Narayan, "The capacity of the arbitrarily varying channel revisited: Positivity, constraints," *IEEE Trans. Inf. Theory*, vol. 34, no. 2, pp. 181–193, Mar. 1988

Detection Framework

- Task of a Turing machine $\mathfrak{T}$ is to **detect denial-of-service attacks**

This is an Entscheidungsproblem, since for a given $\mathfrak{W}$, the Turing machine $\mathfrak{T}$ should answer the question whether or not a denial-of-service attack takes place

- A hypothetical algorithm (or Turing machine) takes all channels $\mathcal{CH}_c(\mathcal{X}, \mathcal{S}; \mathcal{Y})$ and partitions this set into two disjoint subsets
  - $\mathcal{M}_{\text{DoS}}^c$ are those $\mathfrak{W}$ for which $C(\mathfrak{W}) > 0$
  - $\mathcal{M}_{\text{DoS}}$ are those $\mathfrak{W}$ for which a denial-of-service attack is possible, i.e., $\mathfrak{W} \in \mathcal{CH}_c(\mathcal{X}, \mathcal{S}; \mathcal{Y})$ with $C(\mathfrak{W}) = 0$

$$\mathcal{M}_{\text{DoS}} = \{\mathfrak{W} \in \mathcal{CH}_c(\mathcal{X}, \mathcal{S}; \mathcal{Y}) : F(\mathfrak{W}) = 0\}$$

- Since $\mathcal{M}_{\text{DoS}}$ is characterized by the continuous function $F(\cdot)$, the set is well defined

$\Rightarrow$ **Analytically, this is easy to answer! And algorithmically...?**

Question 1: Is there an algorithm (or Turing machine) $\mathfrak{T}$ that takes $\mathfrak{W}$ as an input and **outputs $\mathfrak{T}(\mathfrak{W}) = 1$ if the Jammer is able to perform a denial-of-service attack** and **otherwise outputs $\mathfrak{T}(\mathfrak{W}) = 0$**?

Question 2: Is there an algorithm (or Turing machine) $\mathfrak{T}'$ that takes $\mathfrak{W}$ as an input and **stops if the Jammer is not able to perform a denial-of-service attack**, i.e., whenever $C(\mathfrak{W}) > 0$?

- Framework also important for system evaluation and verification

H. Boche, R. F. Schaefer, and H. V. Poor, "Performance evaluation of secure communication systems on Turing machines," in *Proc. 10th IEEE Int. Workshop Inf. Forensics Security*, Hong Kong, Dec. 2018, pp. 1–7

Computability

- A sequence of rational numbers $\{r_n\}_{n\in\mathbb{N}}$ is called *computable* if there exist recursive functions $a, b, s : \mathbb{N} \to \mathbb{N}$ with $b(n) \neq 0$ for all $n \in \mathbb{N}$ and

$$r_n = (-1)^{s(n)} \frac{a(n)}{b(n)}, \qquad n \in \mathbb{N}$$

- A *real number x is said to be computable* if there exists a computable sequence of rational numbers $\{r_n\}_{n\in\mathbb{N}}$ such that

$$|x - r_n| < 2^{-n} \qquad \text{for all } n \in \mathbb{N}$$

- $\mathbb{R}_c$ is the set of computable real numbers
- $\mathcal{P}_c(\mathcal{X})$ is the set of computable probability distributions (i.e., all $P \in \mathcal{P}(\mathcal{X})$ such that $P(x) \in \mathbb{R}_c$, $x \in \mathcal{X}$)
- $\mathcal{CH}_c(\mathcal{X}; \mathcal{Y})$ is the set of all computable channels (i.e., for $W : \mathcal{X} \to \mathcal{P}(\mathcal{Y})$ we have $W(\cdot|x) \in \mathcal{P}_c(\mathcal{Y})$ for every $x \in \mathcal{X}$)

Definition: A function $f : \mathbb{R}_c \to \mathbb{R}_c$ is called *Borel computable* if there is an algorithm that transforms each given computable sequence of a computable real x into a corresponding representation for $f(x)$.

R. I. Soare, *Recursively Enumerable Sets and Degrees.* Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 1987

Detectability

Theorem: *For all $|\mathcal{X}| \geqslant 2$, $|\mathcal{S}| \geqslant 2$, and $|\mathcal{Y}| \geqslant 2$, there is **no** Turing machine $\mathfrak{T} : \mathcal{CH}_c(\mathcal{X}, \mathcal{S}; \mathcal{Y}) \to \{0, 1\}$ with $\mathfrak{T}(\mathfrak{W}) = 1$ if and only if $\mathfrak{W} \in \mathcal{M}_{\text{DoS}}$.*

- We look for a Turing machine that stops for every channel $\mathfrak{W} \in \mathcal{CH}_c(\mathcal{X}, \mathcal{S}; \mathcal{Y})$ and further $\mathfrak{T}(\mathfrak{W}) = 1$ if and only if $\mathfrak{W} \in \mathcal{M}_{\text{DoS}}$

$\Rightarrow$ Such a Turing machine does **not** exist
$\Rightarrow$ This question is **algorithmically undecidable**!
$\Rightarrow$ This provides a negative answer to Question 1

- Drop requirement of stopping:
- Is there a Turing machine that stops if and only if $\mathfrak{W} \in \mathcal{M}_{\text{DoS}}^c$? Otherwise, the Turing machine may not stop at all

Theorem: *There is a Turing machine $\mathfrak{T} : \mathcal{CH}_c(\mathcal{X}, \mathcal{S}; \mathcal{Y}) \to \{\text{stop}, \text{run forever}\}$ that stops if and only if $\mathfrak{W} \in \mathcal{M}_{\text{DoS}}^c$, i.e., no denial-of-service attack is possible.*

$\Rightarrow$ Such a Turing machine does exist
$\Rightarrow$ This question is **algorithmically semidecidable**!
$\Rightarrow$ This provides a positive answer to Question 2

- A similar approach for $\mathcal{M}_{\text{DoS}}$ (as done for $\mathcal{M}_{\text{DoS}}^c$) is not possible (otherwise it would then be possible to simply run both machines in parallel)

Theorem: *There is **no** Turing machine $\mathfrak{T} : \mathcal{CH}_c(\mathcal{X}, \mathcal{S}; \mathcal{Y}) \to \{\text{stop}, \text{run forever}\}$ that stops if and only if $\mathfrak{W} \in \mathcal{M}_{\text{DoS}}$.*

$\Rightarrow$ This question is **algorithmically not semidecidable**!

Jammer with Full Knowledge

- Jammer knows the actual transmitted message!

$\Rightarrow$ AVC with maximum error for which capacity is unknown

Theorem: *For an AVC $\mathfrak{W}$ under the maximum error criterion, we have $C_{max} > 0$ if and only if there exist $x, \hat{x} \in \mathcal{X}$ with $\mathcal{I}(x) \cap \mathcal{I}(\hat{x}) \neq \emptyset$. with $\mathcal{I}(x) = \{p \in \mathcal{P}(\mathcal{Y}) : \exists q \in \mathcal{P}(\mathcal{S})$ s.t. $p(y) = \sum_{s\in\mathcal{S}} W(y|x, s)q(s)\}$*

R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Z. Wahrscheinlichkeitstheorie verw. Gebiete*, vol. 44, no. 2, pp. 159–175, Jun. 1978

- $\overline{\mathcal{M}}_{\text{DoS}}$ are those $\mathfrak{W}$ for which a denial-of-service attack is possible

Theorem: *For all $|\mathcal{X}| \geqslant 2$, $|\mathcal{S}| \geqslant 2$, and $|\mathcal{Y}| \geqslant 2$, there is **no** Turing machine $\mathfrak{T} : \mathcal{CH}_c(\mathcal{X}, \mathcal{S}; \mathcal{Y}) \to \{0, 1\}$ with $\mathfrak{T}(\mathfrak{W}) = 1$ if and only if $\mathfrak{W} \in \overline{\mathcal{M}}_{\text{DoS}}$.*

Theorem: *There is a Turing machine $\mathfrak{T} : \mathcal{CH}_c(\mathcal{X}, \mathcal{S}; \mathcal{Y}) \to \{\text{stop}, \text{run forever}\}$ that stops if and only if $\mathfrak{W} \in \overline{\mathcal{M}}_{\text{DoS}}^c$, i.e., no denial-of-service attack is possible.*

H. Boche, R. F. Schaefer, and H. V. Poor, "Denial-of-service attacks on communication systems: Detectability and jammer knowledge," 2019, in preparation