

On the Need of Neuromorphic Twins to Detect Denial-of-Service Attacks on Communication Networks

Holger Boche* (BO 1734/42-1), Rafael Schaefer† (SCHA 1944/11-1), H. Vincent Poor‡, Frank H. P. Fitzek† (FI 1671/10-1)

* Technische Universität München

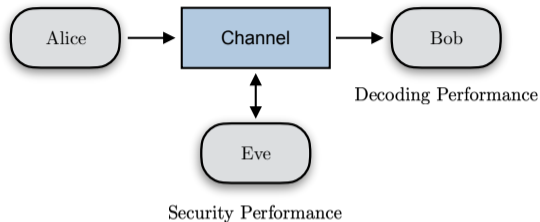
† Technische Universität Dresden

‡ Princeton University

Resilient Worlds Status Update Meeting

July 4-5, 2024

Motivation: Denial of Service as Security Attack



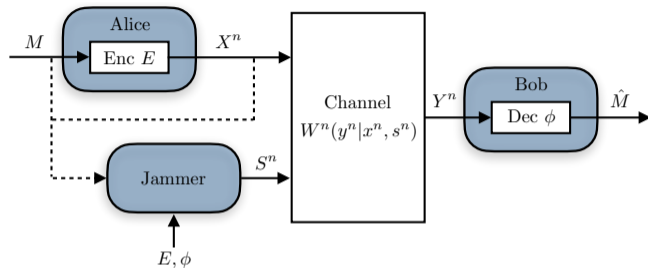
Attack strategies of Eve:

- Security \Rightarrow quantum computer \Rightarrow **very expensive**
- Communication / decoding performance – Denial of Service \Rightarrow **inexpensive**

very expensive attacks on security mechanisms vs inexpensive jamming attacks

As a consequence, we need **resilience by design!**

Communication System with a Jammer



- 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

$$W^n(y^n|x^n, s^n) = \prod_{i=1}^n W(y_i|x_i, s_i)$$

- *Jammer with Partial Knowledge* knows encoder E and decoder ϕ
- *Jammer with Full Knowledge* additionally knows actual message M (or $X^n = X^n(M)$)

Denial-of-Service (DoS) Attacks

- Goal of the Jammer: Successfully launch a DoS attack
- We are interested in studying **DoS attacks**, where the Jammer is able to completely **disrupt the communication**
 - Whatever decoding strategy the receiver may use and computational capabilities the receiver may have, it is **not able to decode the transmitted message**
- Such DoS attacks can be
 - unintentionally due to high interference coming from other (uncoordinated) transmitters or
 - intentionally due to jamming attacks from active adversaries
- The traditional approach of **detecting such attacks and reacting to those is realized on higher layers** based on channel state information (such as SINR, RSS, ...) and may further be integrated into the resource allocation

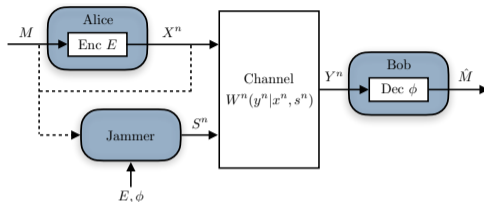
Denial-of-Service (DoS) Attacks (2)

Question: Is it possible at all to realize detection of (and subsequent reaction to) DoS attacks on higher layers?

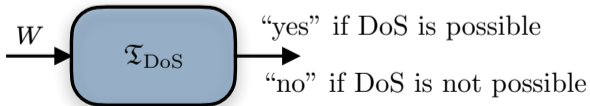
- Particularly relevant as there is a recent trend towards realizing functionalities in software only (such as *software-defined networking (SDN)* and *network function virtualization (NFV)*)

How can we formalize this in a precise and rigorous way?

Detection of DoS Attacks via Turing Machines



Problem formulation: Is the question *"Is the Jammer able to perform a DoS attack?"* decidable by a Turing machine? Is there a Turing machine $\mathfrak{T}_{\text{DoS}}$ such that



Properties of DoS Attacks

- Let \mathcal{X} , \mathcal{Y} , and \mathcal{S} be the input, output and state sets
- Let \mathcal{M}_{DoS} the set of all channels for which a DoS attack is possible

Theorem:

[BSP 2020]

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



H. Boche, R. F. Schaefer, and H. V. Poor, “Denial-of-service attacks on communication systems: Detectability and jammer knowledge,” *IEEE Trans. Signal Process.*, vol. 68, pp. 3754–3768, 2020

Feedback does **not** help – detection problem remains undecidable on Turing machines



—, “On the algorithmic solvability of channel dependent classification problems in communication systems,” *IEEE/ACM Trans. Netw.*, vol. 29, no. 3, pp. 1155–1168, Jun. 2021

Blum-Shub-Smale (BSS) Machines

- It can store *arbitrary real numbers*, can compute all field operations on \mathbb{R} , i.e., “+” and “·”, and can compare real numbers according to the relations “<”, “>”, and “=”
- A BSS machine is similar to a Turing machine in the sense that it operates on an infinite strip of tape according to a so-called program. This is a finite directed graph with five types of nodes associated with different operations: input node, computation node, branch node, shift node, and output node

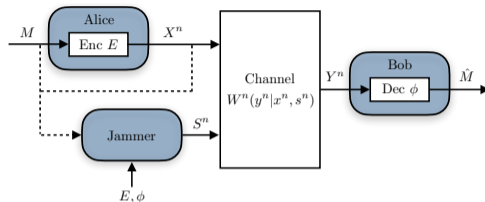
BSS-computable functions are input-output maps Φ of the BSS machine \mathfrak{B} , i.e., for every input \mathbf{x} , the output $\Phi_{\mathfrak{B}}(\mathbf{x})$ is defined if the output is reachable by the program of \mathfrak{B} .

A set $\mathcal{A} \subset \mathbb{R}^N$ is *BSS-decidable* if there is a BSS machine $\mathfrak{B}_{\mathcal{A}}$ such that for all $\mathbf{x} \in \mathbb{R}^N$ we have $\mathfrak{B}_{\mathcal{A}}(\mathbf{x}) = \chi_{\mathcal{A}}(\mathbf{x})$, i.e., the characteristic function $\chi_{\mathcal{A}}$ of the set \mathcal{A} is BSS-computable.

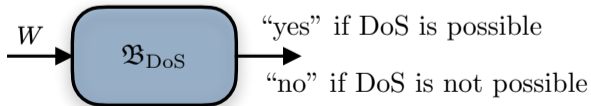


L. Blum, M. Shub, and S. Smale, “On a theory of computation and complexity over the real numbers: *NP*-completeness, recursive functions and universal machines,” *Bull. Amer. Math. Soc.*, vol. 21, no. 1, pp. 1–46, Jul. 1989

Detection of DoS Attacks via BSS Machines



Problem formulation: Is the question *"Is the Jammer able to perform a DoS attack?"* decidable by a BSS machine? Is there a BSS machine $\mathfrak{B}_{\text{DoS}}$ such that



DoS Attacks with Blum-Shub-Smale Machines

Theorem:

Let \mathcal{X} , \mathcal{Y} , and \mathcal{S} be arbitrary finite alphabets. Then there exists a BSS machine \mathfrak{B} that outputs $\mathfrak{B}(W) = \text{“yes”}$ if and only if $W \in \mathcal{M}_{\text{DoS}}$, i.e., the DoS detection problem is BSS-decidable.

Main proof ingredient:

- Exploit connections to the theory of semialgebraic sets
 - Show that both sets \mathcal{M}_{DoS} and $\mathcal{M}_{\text{DoS}}^c$ are semialgebraic
- ▣ The result remains **true** also in case where the Jammer also knows the transmitted message, i.e., the most powerful jammer

Conclusions

- *Detection framework based on Turing machines*
 - Turing machines provide fundamental performance limits for today's digital computers and therewith of traditional signal processing
 - Turing machines are **not capable of detecting DoS attacks!**
 - **Feedback does not help** – detection problem remains undecidable
- *Detection framework based on BSS machines*
 - Allows the processing and storage of arbitrary reals
 - BSS machines are **capable of detecting DoS attacks!**
 - Real number signal processing enables the detection of DoS attacks

▸ Solution to the DoS detectability problem: **Computing model** is very important!



H. Boche, R. F. Schaefer, H. V. Poor, and F. H. P. Fitzek, "On the need of neuromorphic twins to detect denial-of-service attacks on communication networks," *IEEE/ACM Trans. Networking*, pp. 1–13, 2024, early access

Thank you for your attention!

Supported by







Deutsche
Forschungsgemeinschaft

German Research Foundation



BO 1734/42-1
SCHA 1944/11-1
FI 1671/10-1

References

-  H. Boche, R. F. Schaefer, and H. V. Poor, “Denial-of-service attacks on communication systems: Detectability and jammer knowledge,” *IEEE Trans. Signal Process.*, vol. 68, pp. 3754–3768, 2020.
-  —, “On the algorithmic solvability of channel dependent classification problems in communication systems,” *IEEE/ACM Trans. Netw.*, vol. 29, no. 3, pp. 1155–1168, Jun. 2021.
-  L. Blum, M. Shub, and S. Smale, “On a theory of computation and complexity over the real numbers: *NP*-completeness, recursive functions and universal machines,” *Bull. Amer. Math. Soc.*, vol. 21, no. 1, pp. 1–46, Jul. 1989.
-  H. Boche, R. F. Schaefer, H. V. Poor, and F. H. P. Fitzek, “On the need of neuromorphic twins to detect denial-of-service attacks on communication networks,” *IEEE/ACM Trans. Networking*, pp. 1–13, 2024, early access.