Internet security in the quantum era

Joaquin Garcia-Alfaro

IMT/Télécom SudParis

LINCS - Atelier residentiel (Immersive workshop), 17/12/2025

Qui suis-je ?

https://j.mp/jgalfaro

- **IMT depuis 2010 (IMT-Atlantique)**

  « Sécurité, réseaux spontanés et systèmes de détection d'intrusions »

- **Depuis 2013 à Télécom SudParis (TSP)**

  - « Poste professeur en cybersécurité »
  - Responsable équipe SCN (Sécurité et Confiance Numérique) à TSP & axe 4 centre RSTN

Qui suis-je ?

https://j.mp/jgalfaro

- **IMT depuis 2010 (IMT-Atlantique)**

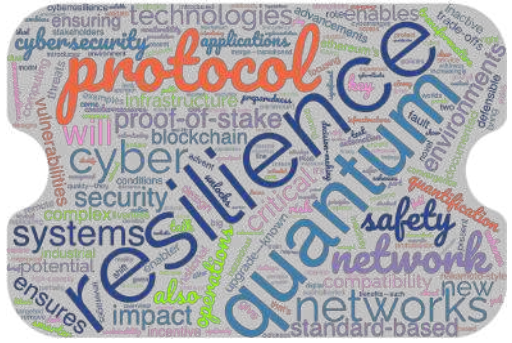
  « Sécurité, réseaux spontanés et systèmes de détection d'intrusions »

- **Depuis 2013 à Télécom SudParis (TSP)**

  - « Poste professeur en cybersécurité »
  - Responsable équipe SCN (Sécurité et Confiance Numérique) à TSP & axe 4 centre RSTN

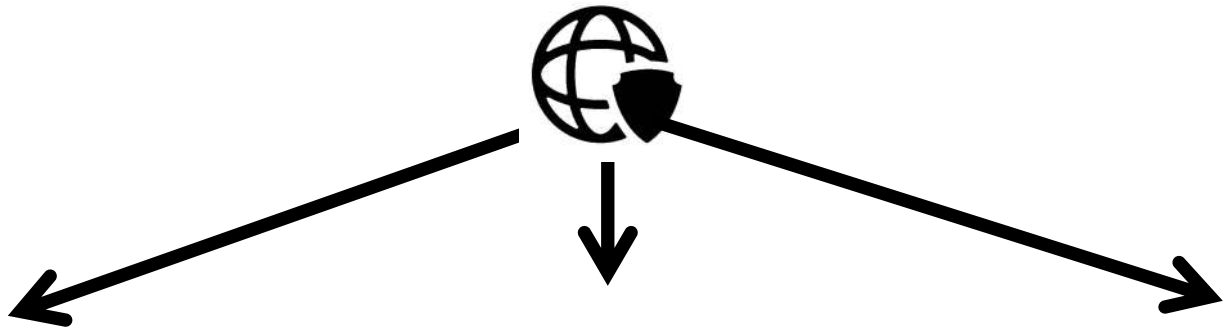
https://scn.telecom-sudparis.eu/

Nos travaux de recherche (SCN & Axe 4 RSTN)



https://centre-rstn.wp.imt.fr/axe-4/

Nos travaux de recherche



Protection

(avant l'attaque)

Cryptography,
Security Protocols,
Access Control,
Security Policies,
Privacy Regulation,
Anonymization, ...

Défense

(pendant l'attaque)

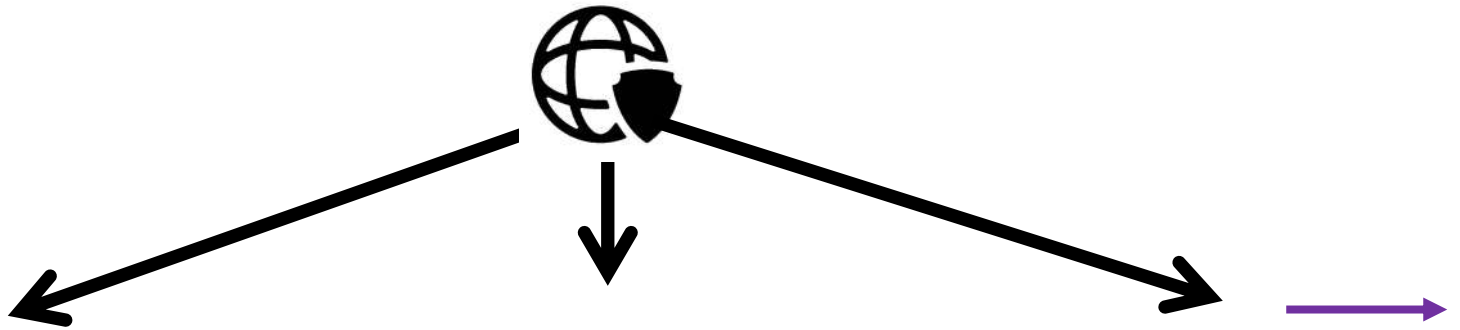
Monitoring, Audit,
Malware Detection,
Alert Correlation,
System Diagnosis, ...

Résilience

(après l'attaque)

Metrics & Deception,
Moving Target Strategies,
Game-Theory, Consensus,
Decentralization, ...

Nos travaux de recherche



Protection

(avant l'attaque)

Cryptography,
Security Protocols,
Access Control,
Security Policies,
Privacy Regulation,
Anonymization, ...

Défense

(pendant l'attaque)

Monitoring, Audit,
Malware Detection,
Alert Correlation,
System Diagnosis, ...

Résilience

(après l'attaque)

Metrics & Deception,
Moving Target Strategies,
Game-Theory, Consensus,
Decentralization, ...

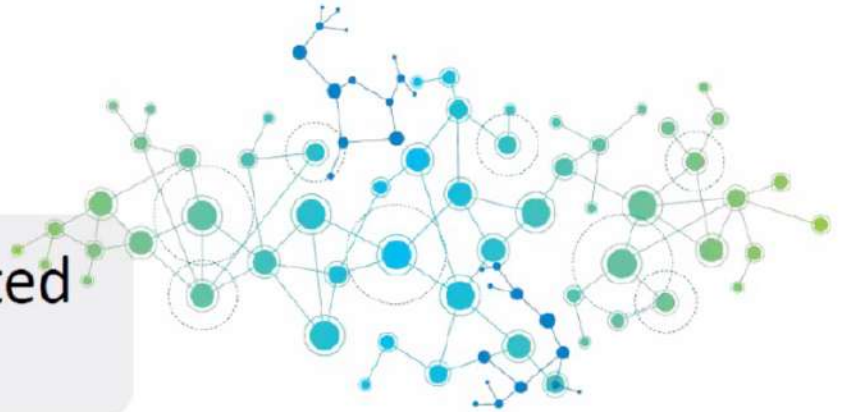
(Cyber) Résilience?

Resilience: ability of a system to provide a satisfactory service level in the face of disruptive events

How resilient is Internet? Would it change due to, e.g., Q-day (quantum as a threat)?

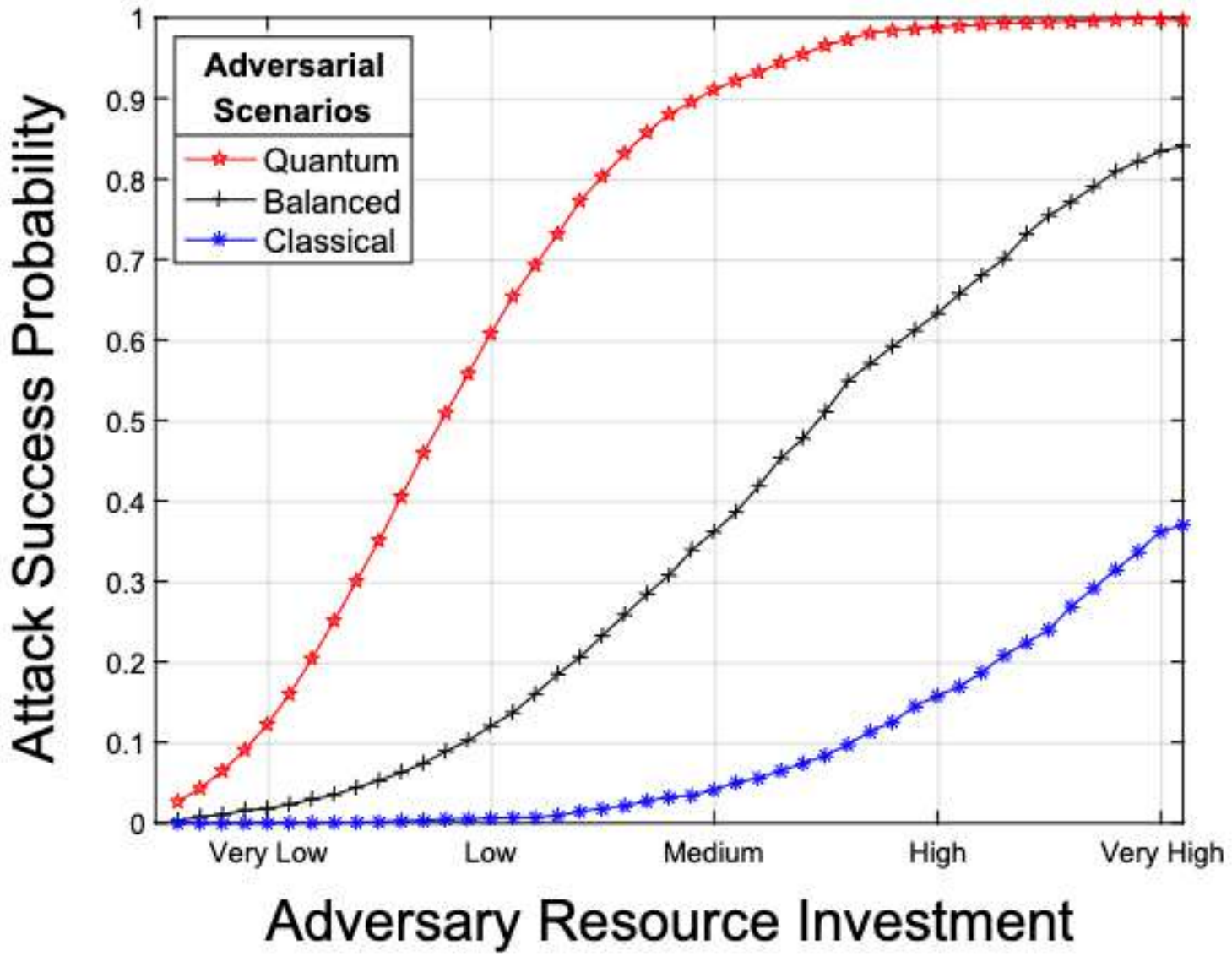
Functional metrics (Performance-related)

Structure-related metrics



Lewis, Ted G. *The many faces of resilience.* Communications of the ACM, 2022.

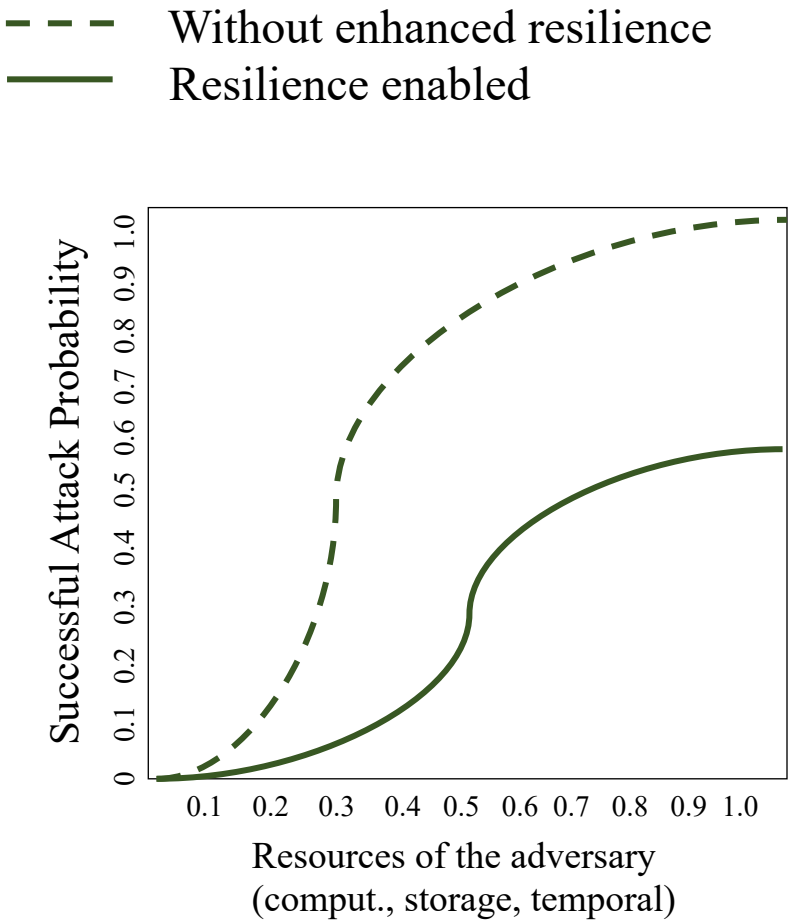
Défis actuels*



* Barbeau, Garcia-Alfaro et al.. The Quantum What? Advantage, Utopia or Threat? *Digitale Welt*, 4:34-39, October 2021.

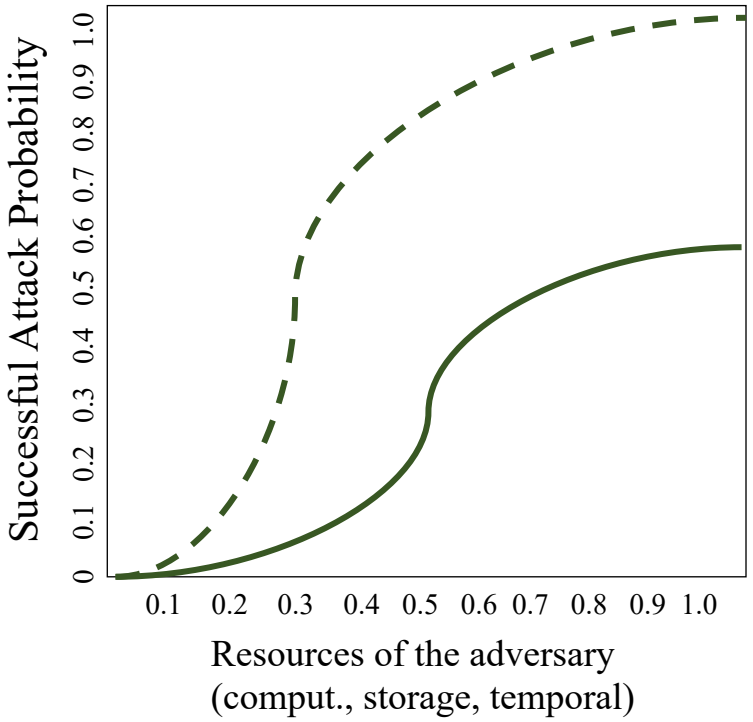
* Barbeau & Garcia-Alfaro. Cyber-Physical Defense in the Quantum Era. Scientific Reports, 12(1):1905, February 2022.

Travaux en cours



Travaux en cours

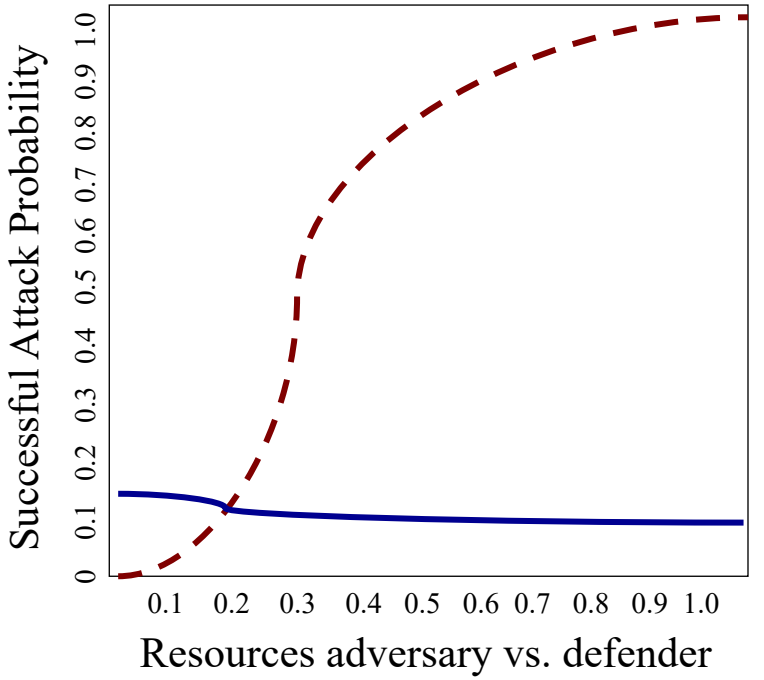
Without enhanced resilience
Resilience enabled



Resilience Disabled

Attacking the system (dashed red curve) is proportional to the resources of the adversary

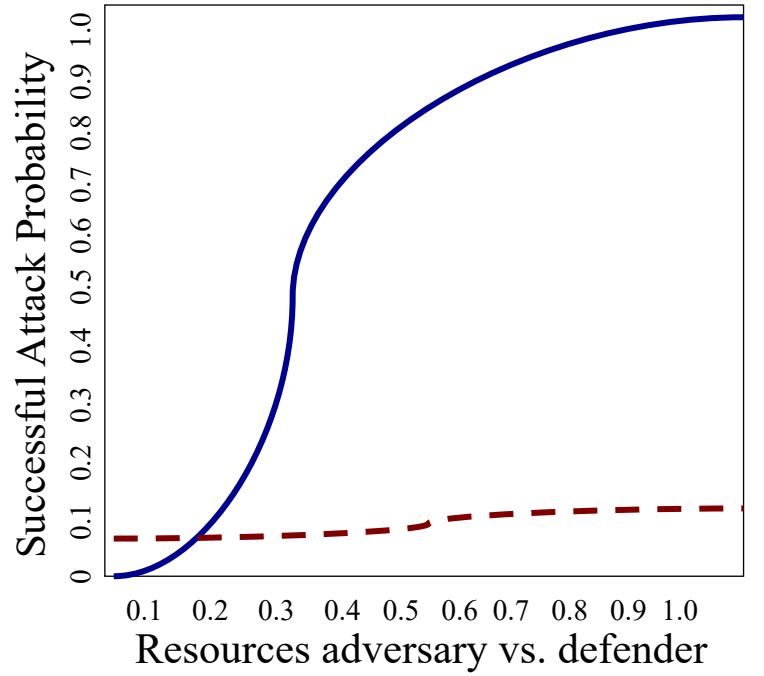
Defending the system (solid blue curve) is harder than attacking the system



Resilience Enabled

Attacking the system (dashed red curve) is non-proportional to the resources of the adversary, anymore

Defending the system (solid blue curve) is easier than attacking the system

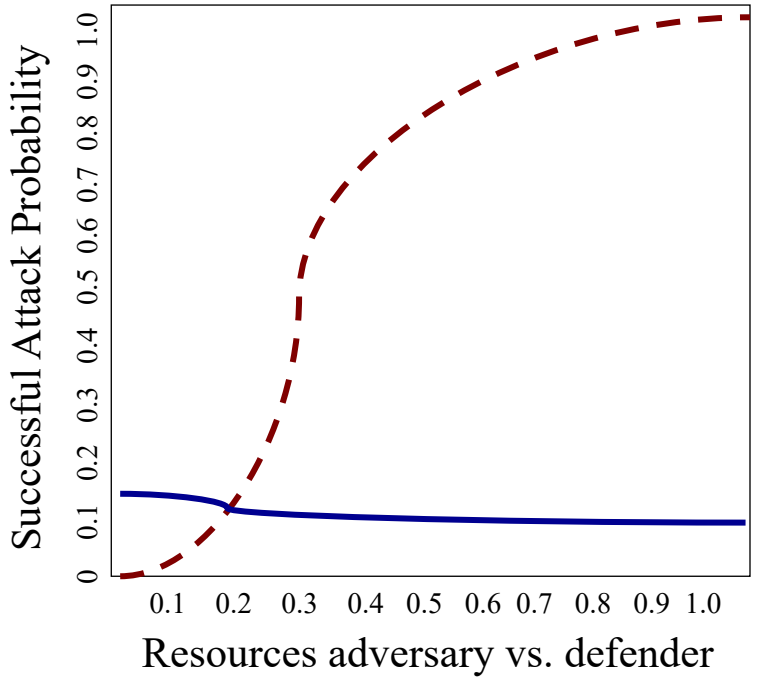


Objectif final

Resilience Disabled

Attacking the system (dashed red curve) is proportional to the resources of the adversary

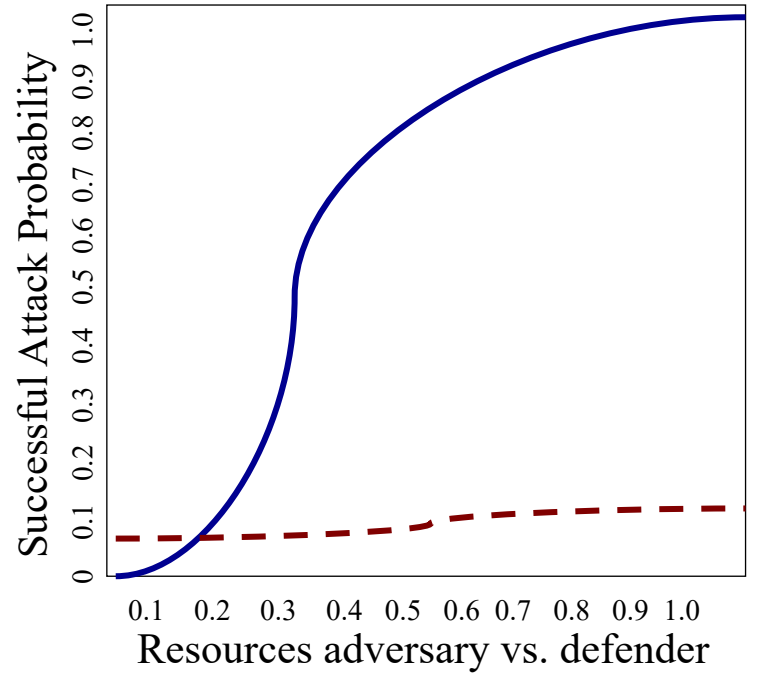
Defending the system (solid blue curve) is harder than attacking the system



Resilience Enabled

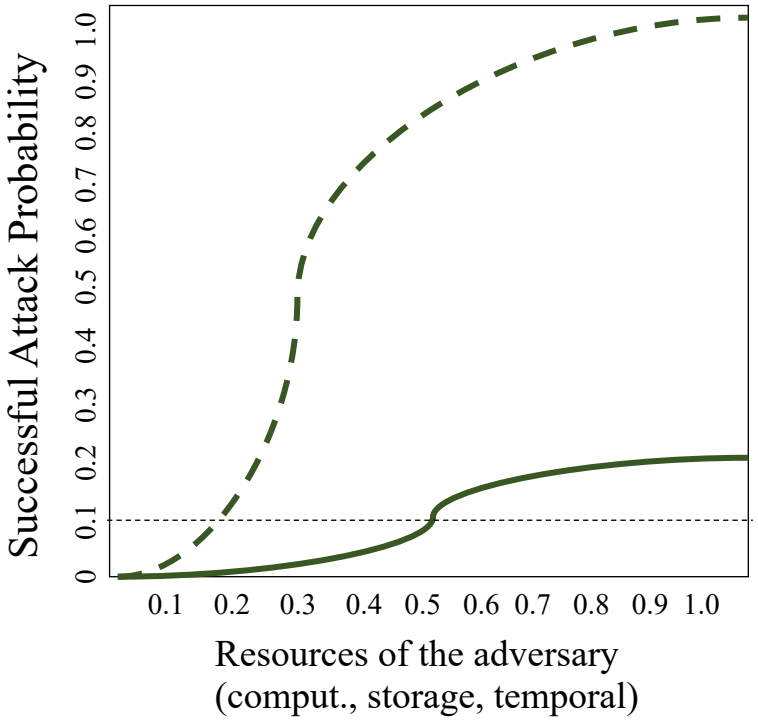
Attacking the system (dashed red curve) is non-proportional to the resources of the adversary, anymore

Defending the system (solid blue curve) is easier than attacking the system



Objectif final

Without enhanced resilience
Resilience enabled

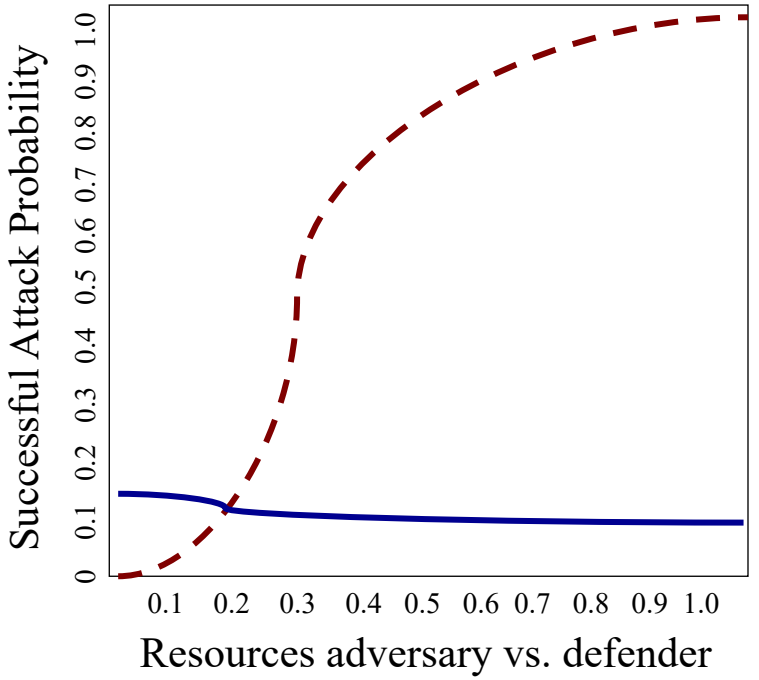


Brute-force level

Resilience Disabled

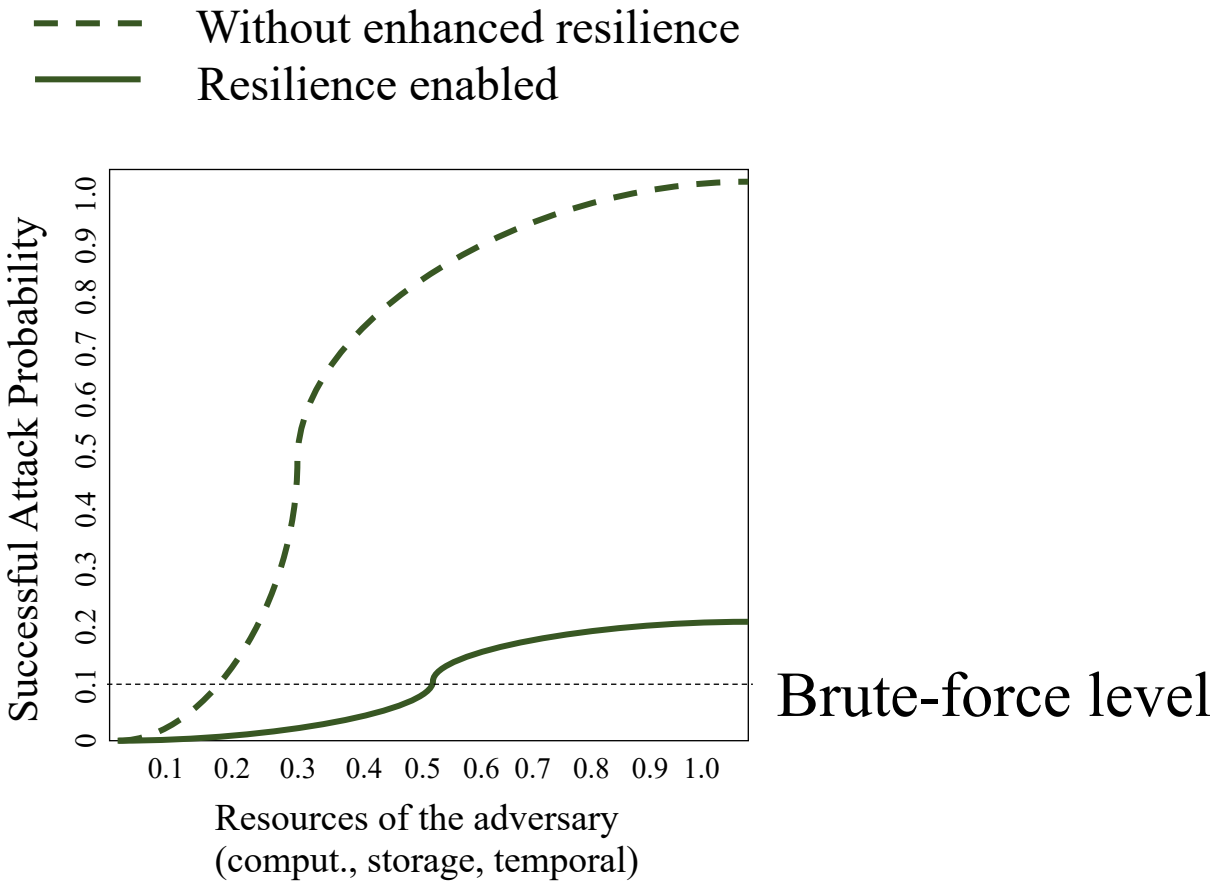
Attacking the system (dashed red curve) is proportional to the resources of the adversary

Defending the system (solid blue curve) is harder than attacking the system



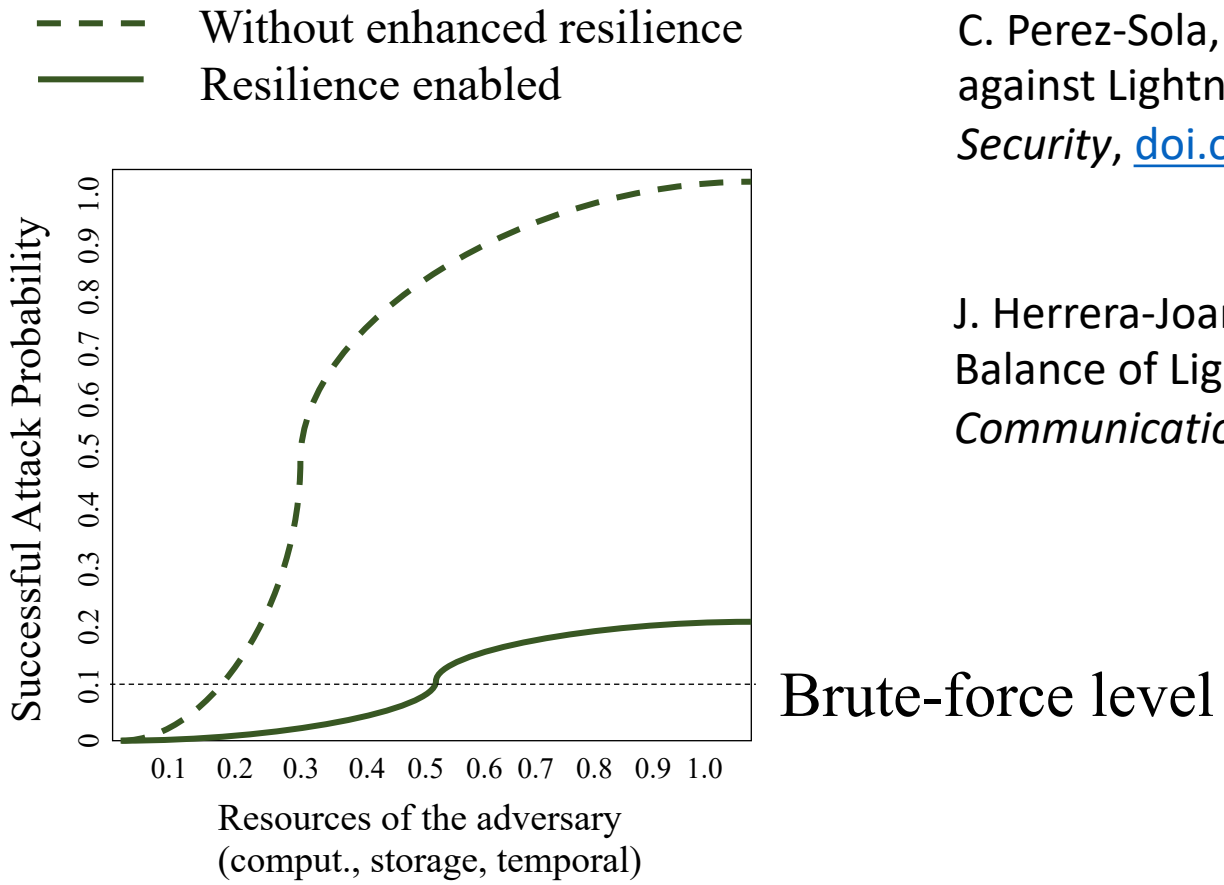
- Make the attack unaffordable to powerful adversaries
- I.e., reduce the likelihood of the attack by increasing the cost

Objectif final



- Make the attack unaffordable to powerful adversaries
- I.e., reduce the likelihood of the attack by increasing the cost

Objectif final



Brute-force level

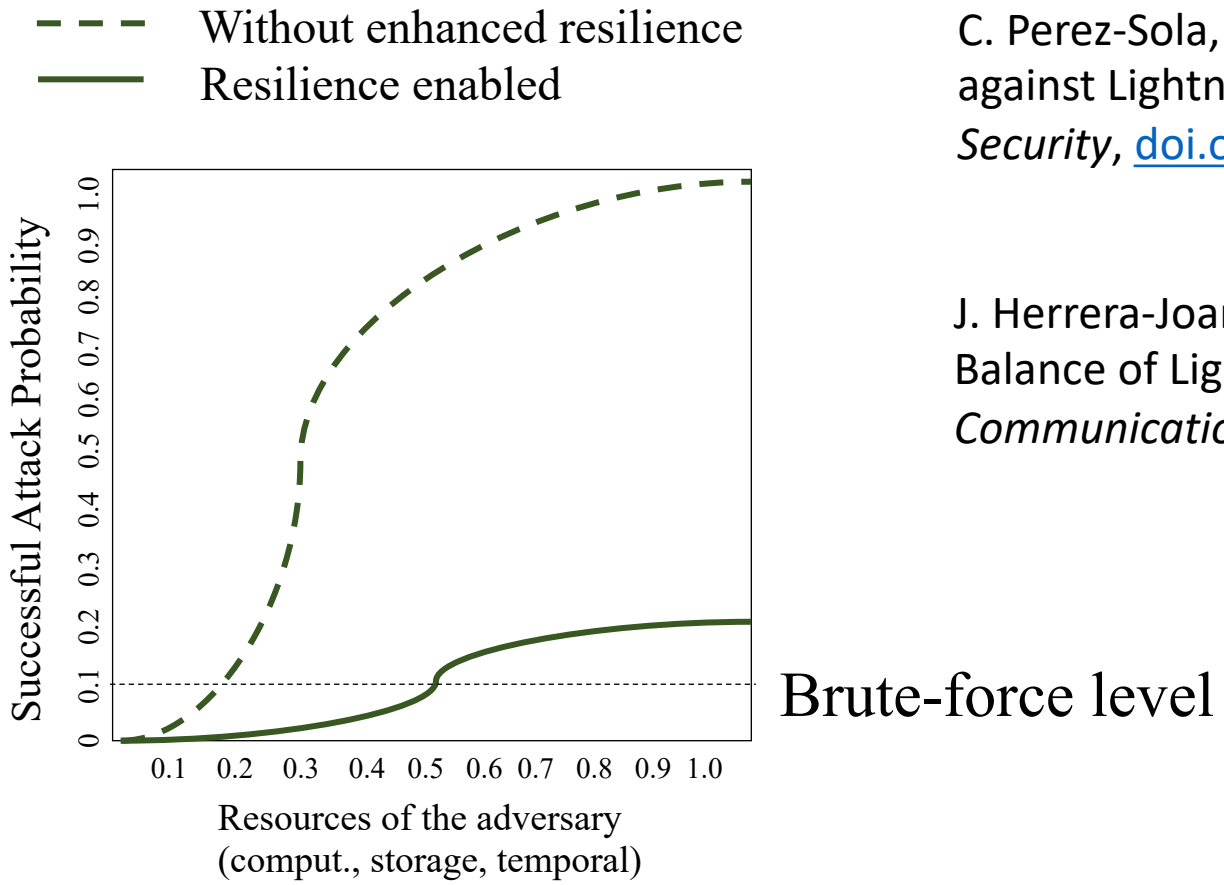
- Make the attack unaffordable to powerful adversaries
- I.e., reduce the likelihood of the attack by increasing the cost

Two sample publications:

C. Perez-Sola, J. Garcia-Alfaro, et al. "LockDown: Balance Availability Attack against Lightning Network Channels". *Financial Cryptography and Data Security*, doi.org/10.1007/978-3-030-51280-4_14

J. Herrera-Joancomarti, J. Garcia-Alfaro, et al. "On the Difficulty of Hiding the Balance of Lightning Network Channels". *14th ACM Asia CCS (Computer and Communications Security)*, doi.org/10.1145/3321705.3329812

Objectif final



Brute-force level

- Make the attack unaffordable to powerful adversaries
- I.e., reduce the likelihood of the attack by increasing the cost

Two sample publications:

C. Perez-Sola, J. Garcia-Alfaro, et al. "LockDown: Balance Availability Attack against Lightning Network Channels". *Financial Cryptography and Data Security*, doi.org/10.1007/978-3-030-51280-4_14

J. Herrera-Joancomarti, J. Garcia-Alfaro, et al. "On the Difficulty of Hiding the Balance of Lightning Network Channels". *14th ACM Asia CCS (Computer and Communications Security)*, doi.org/10.1145/3321705.3329812

Merci.

Questions ?

BACKUP

Satoh et al. Paper (The Network Impact of Hijacking a Quantum Repeater)

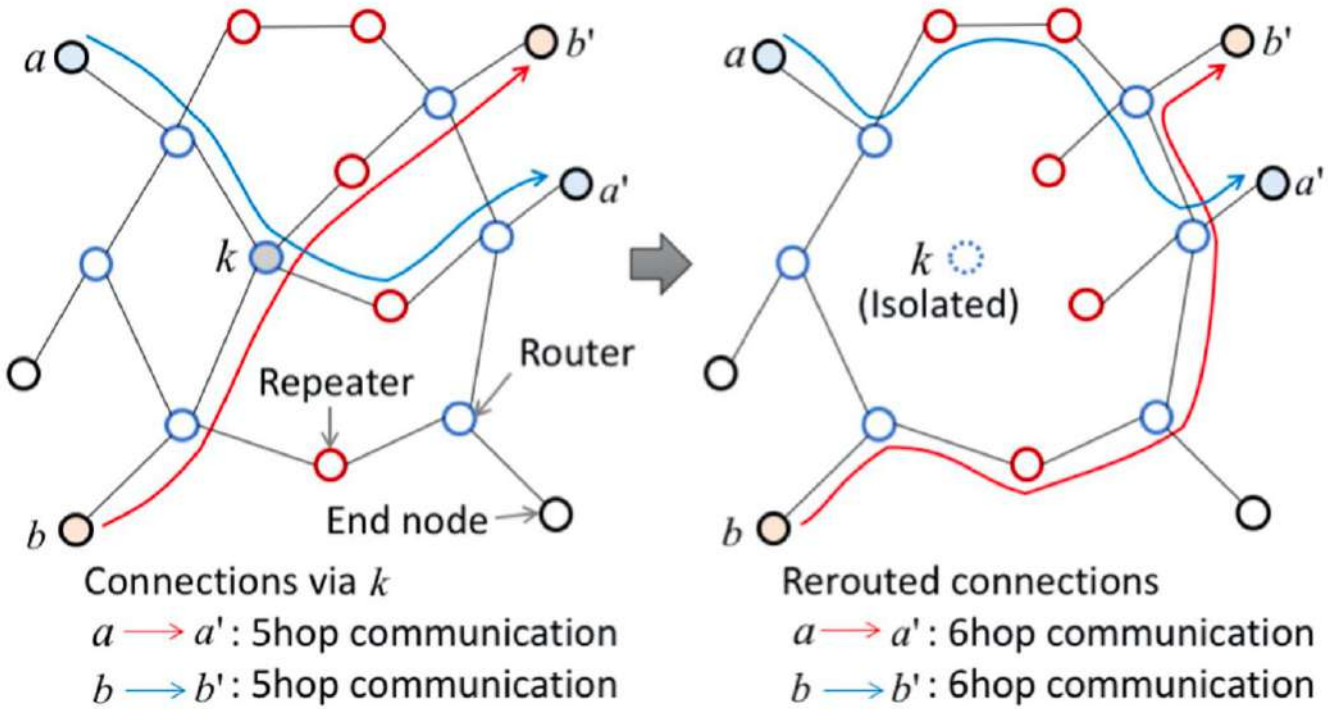


Figure. After detection of *k (hijacked repeater)*, the network isolates *k* and the connections passing through *k* are rerouted.

Contribution:

- *Detection-Reaction* approach
  - Detect, then isolate hijacked repeaters
  - Approach included in the tomography process (i.e., in addition to error monitoring, we can now discover & isolate hijacked repeaters)

Limitation:

- Collateral damage of the reaction approach
  - Adversary can now frame innocent repeaters & isolate them from the network
- Authors don't quantify cost of the attack
- Advantage of quantifying the attack
  - Make the attack unaffordable to average adversaries
  - I.e., we can reduce the likelihood of the attack by increasing the cost (for instance, using the new ideas by Nick in the ACM paper).

Takahiko Satoh[1,3], Shota Nagayama[2], Takafumi Oka[1] and Rodney Van Meter[1]

Quantifying attack costs in terms of resources

- If the attack is affordable, make it less affordable (e.g., use of Clifford operators & Symplectic groups)
  - By affordable, we refer to situations where the resources required by the adversary to perpetrate the attack are much lower than the resources affected by the attack (i.e., impact to the system)
- Examples:
  a) Situation 1: each qubit of the adversary affects n qubits of a path of length n, where $n > 1$
  b) Situation 2: attack gets augmented due to routing loops, so that each qubit of the adversary affects $m \cdot n$ qubits, where m represents number of iterations due to routing loops

Quantifying attacks using **effort ratio** metrics

$$\textbf{AER} = \frac{\text{resources needed to perpetrate the attack}}{\text{affected resources (in the network) after perpetrating the attack}}$$

AER (Attack Effort Ratio) represents the resources needed to perform the attack (e.g., entanglement resources of the adversary) vs. the number of resources affected by the attack (i.e., total number of affected states in the network)

E.g., adding **time** to the analysis ...

In addition to computing the **effort ratio**, we could also consider

> $\Delta(t)$ **function**: e.g., time-based decreasing function that measures the impact of the attack w.r.t. amount of time since the attack was perpetrated

The attack is unaffordable if:

- AER = 1 (i.e., the attack is like a brute-force attack)
- $\Delta(t_0)$ = network affected, but $\Delta(t_1)$ = network unaffected

We can also use the following function:

- Total Exhaustion Time (TET) = $\sum_{b=0}^{\infty} \Delta(t)$

and evaluate cases in which the attack is realistic by

- Minimizing the AER
- Maximizing TET

Sample Attacks

Analyze attacks using concrete applications (e.g., QKD, leader election, QML, ...) to quantify the impact of the attacks (e.g., in the case of leader election, elected nodes are always under the control of the adversary)

Classification of Quantum Repeater Attacks

Shigeya Suzuki*†, Rodney Van Meter‡
*Graduate School of Media and Governance, Keio University, Kanagawa, Japan
†Auto-ID Lab Japan, Keio Research Institute at SFC, Keio University, Kanagawa, Japan
E-mail: shigeya@wide.ad.jp
‡Faculty of Environment and Information Studies, Keio University, Kanagawa, Japan
E-mail: rdv@sfc.wide.ad.jp

***Abstract*—The main service provided by the coming Quantum Internet will be creating entanglement between any two quantum nodes. We discuss and classify attacks on quantum repeaters, which will serve roles similar to those of classical Internet routers. We have modeled the components for and structure of quantum repeater network nodes. With this model, we point out attack vectors, then analyze attacks in terms of confidentiality, integrity and availability. While we are reassured about the promises of quantum networks from the confidentiality point of view, we observe that the requirements on the classical computing/networking elements affect the systems' overall security risks. This component-based analysis establishes a framework for further investigation of network-wide vulnerabilities.**

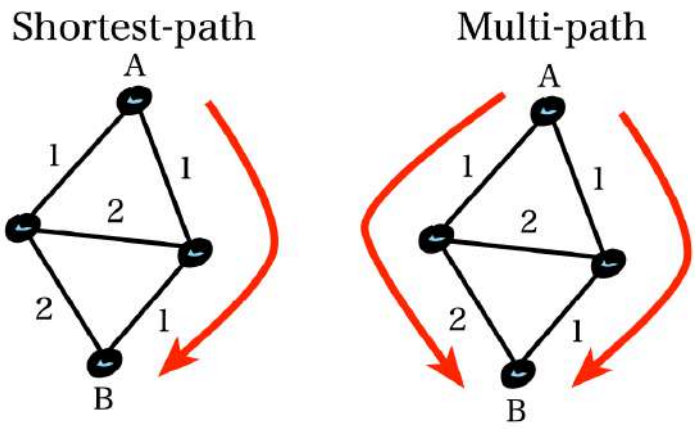
that depend on the difficulty of certain computational problems, but conversely distributed security-related functions such as Byzantine agreement and secret sharing recoup some of the losses [5], [12]. Recently, Broadbent *et al.* developed a fully blind method of conducting any arbitrary quantum calculation [8], [9]. Unlike Gentry's classical homomorphic encryption [14], this technique hides the algorithm itself as well as the input and output data. Thus, if we can find ways of distributing quantum information over long distances, we will enable valuable new functionality.

Cost functions

- ACM paper (attack model)

Is a replay attack possible? Given the no-cloning theorem, it is not possible taking an exact copy of a quantum state and replaying it at a later time. It is however possible for an adversary to delay the delivery of a quantum state to its destination. Assuming that the adversary has the information, it can also recreate and replay the quantum state $|\psi\rangle$. In $|\psi\rangle$, there is no mechanism that can be used by the destination to verify that the quantum state is new and has never been received before.

- QuNet paper:



- Multi-path entanglement routing can be considered conceptually similar to the classical notion of *load balancing*, whereby instead of maximising bandwidth by distributing data-packets via redundant routes, we are engaging in *decoherence balancing* by distributing entanglement via redundant routes and subsequently purifying them into one.

Qunet Paper (cost functions)

Paper at: https://arxiv.org/abs/2105.00418

Simulator at: https://peterrohde.github.io/QuNet/

- Use of a cost vector methodology
- Rather than track quantum states themselves, they track the associated costs of each state as they traverse the network
    - Costs are arbitrary properties that accumulate additively as qubits traverse networks
    - Tracking the accumulation of costs acting on Bell pairs is equivalent to directly tracking the states themselves

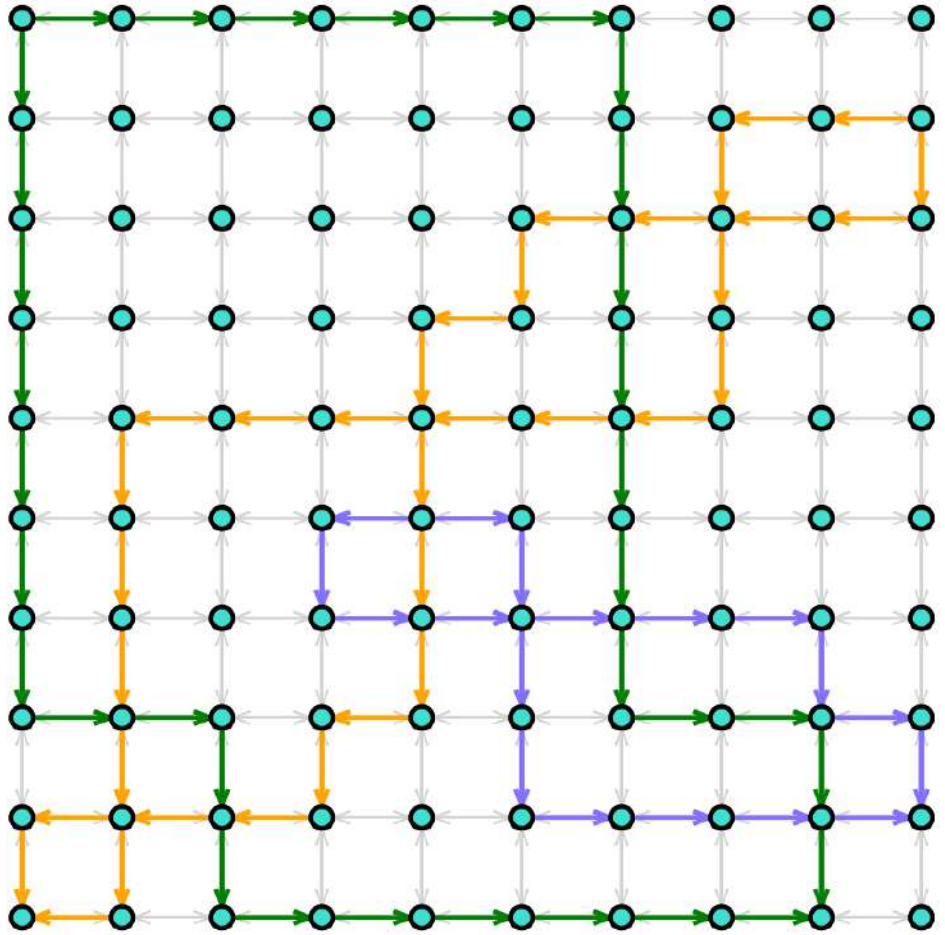


Figure 10: Example execution of the greedy multi-user, multi-path routing algorithm for 3 user-pairs on a 10×10 lattice. Colour coding denotes which channels are allocated to which user-pairs by the algorithm. For each user-pair, resultant paths are finally purified together, yielding end-to-end entanglement links of higher fidelity than the individual shortest-paths. Fig. 19 provides a similar example for multi-user temporal routing.

Qunet Paper (cost functions)

Paper at: https://arxiv.org/abs/2105.00418

Simulator at: https://peterrohde.github.io/QuNet/

- Multi-path entanglement routing: purifying multiple noisy entangled states into a single state, of higher quality ← ***including states from the adversaries?***

- By quantifying the effects of noisy channels on states with additive cost-metrics, they obtain equivalent functionality than frameworks like QUISP (i.e., **multi-user routing & congestion avoidance using quantum memories)**.

- The cost vector approach in the paper (& simulator) could help us to experiment with the AER/TET metrics (Attack Effort Ratio metric & Total Exhaustion Time).

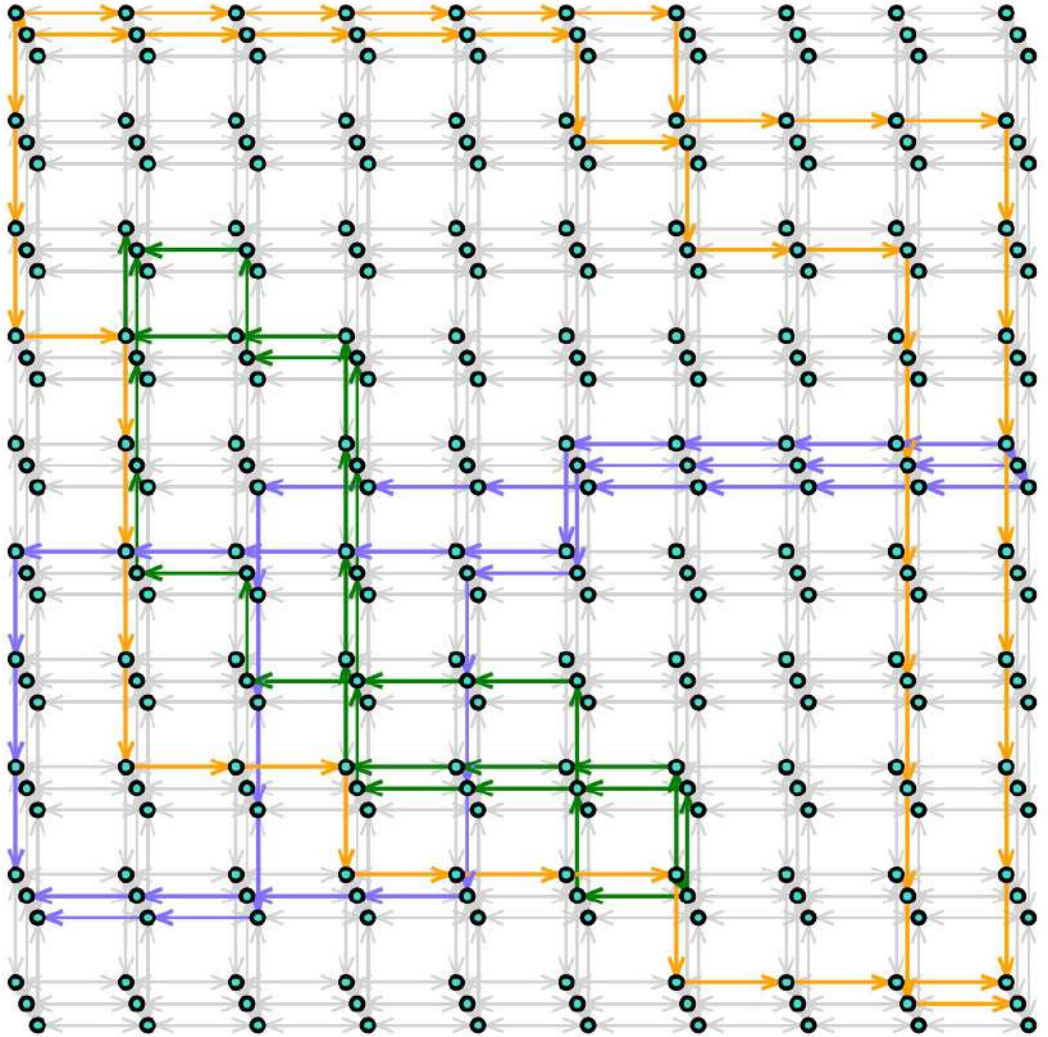
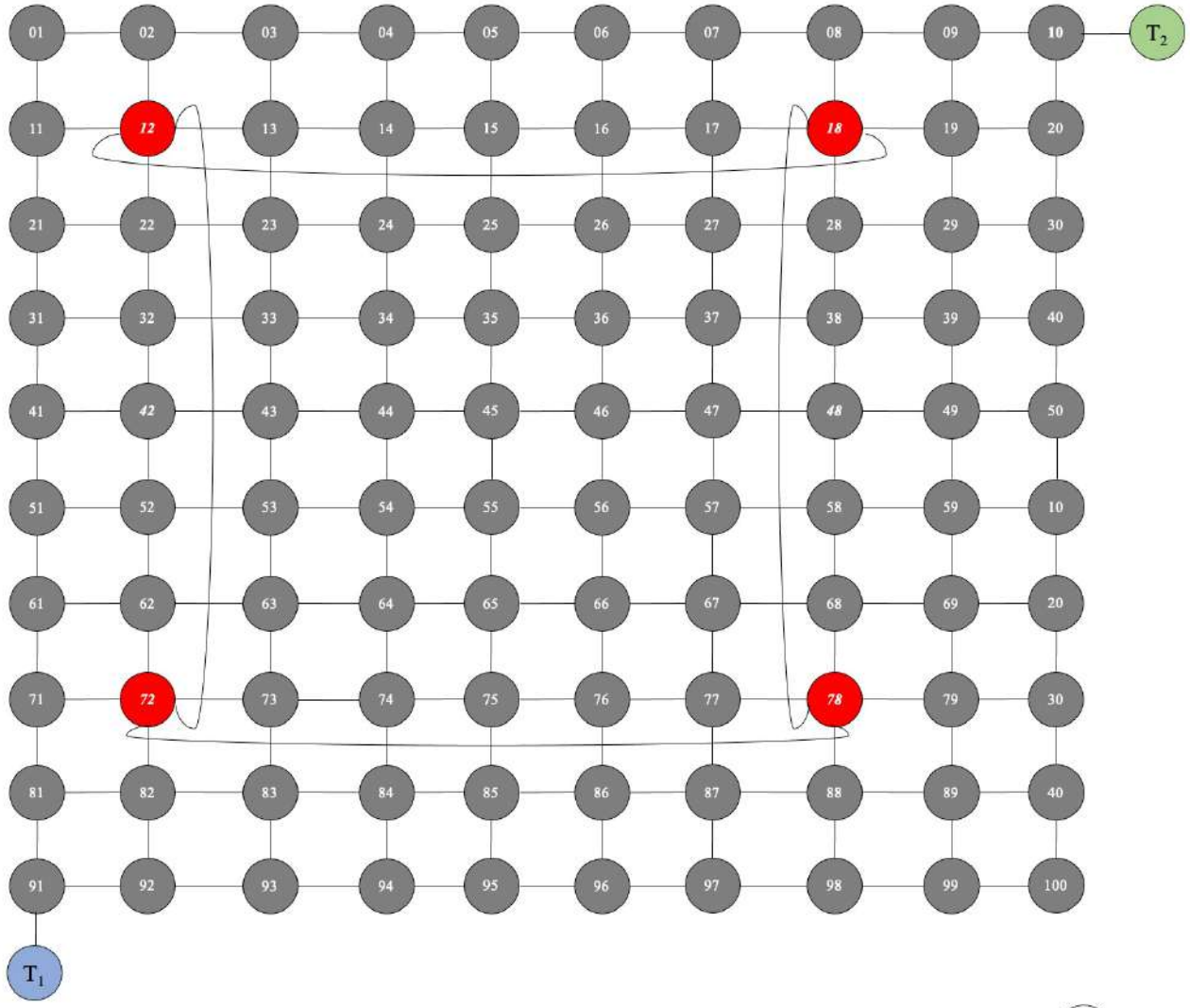


Figure 19: Example of multi-user, multi-path temporal routing with 3 temporal steps (stacked). Utilised channels are colour coded according to which user-pair they serve.



- Deliver a message from terminal T_1 (blue) to terminal T_2 (green)
  - Path 1: T_1, 91, 92, 93, ..., 100, 40, 30, ... , 10, T_2
  - Path 2: T_1, 91, 81, 71, ..., 01, 02, 03, 04, ... , 10, T_2
  - ...
  - Path *k*: T_1, 91, 92, 82, [72, 12, 18, 78], 19, 20, 10, T_2

T_i terminal

i repeater

j hijacked repeater

$[j_1, ..., j_n]$ loop

Network Impact of Hijacking Quantum Repeaters

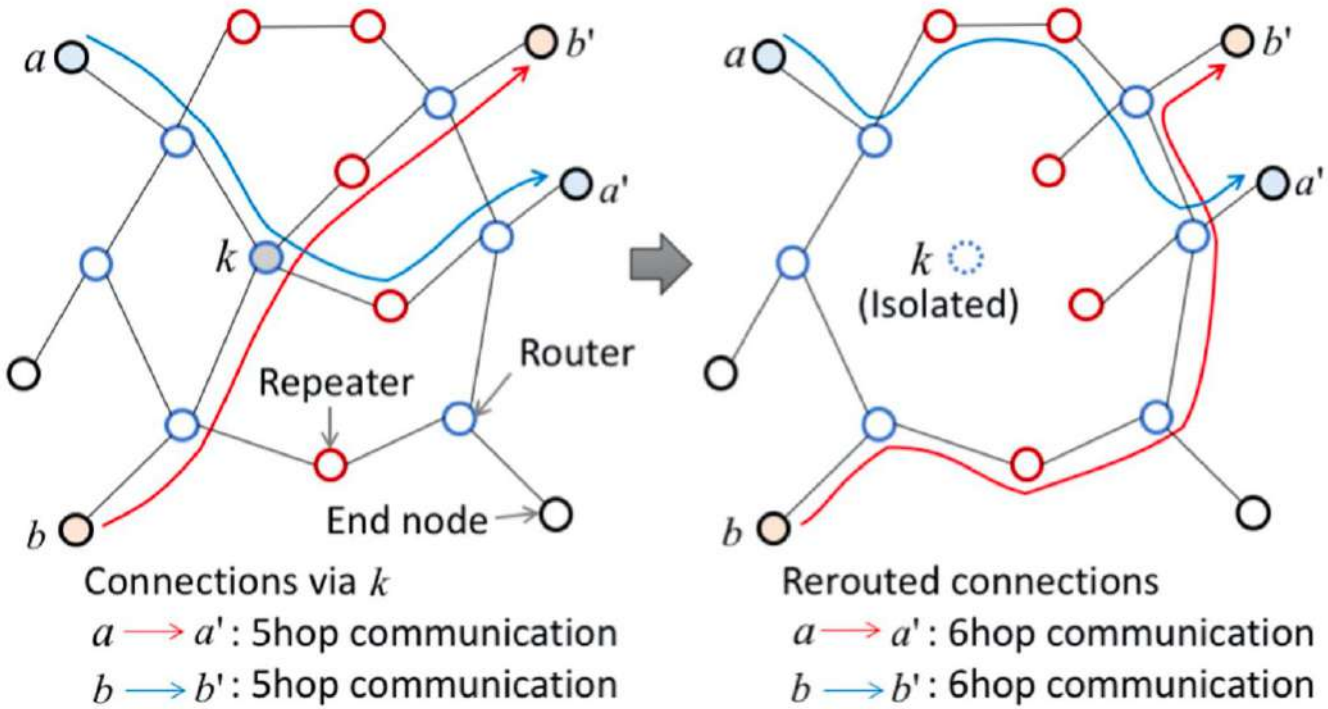


Figure. After detection of *k (hijacked repeater)*, the network isolates *k* and the connections passing through *k* are rerouted.

Takahiko Satoh[1,3], Shota Nagayama[2], Takafumi Oka[1] and Rodney Van Meter[1]

Paper 1, The Network Impact of Hijacking a Quantum Repeater

Figure. After detection of *k (hijacked repeater)*, the network isolates *k* and the connections passing through *k* are rerouted.

Contribution:

- Detection-Reaction approach to discover hijacked repeaters & isolate them
- The approach is included in the tomography process (in addition to error monitoring, we can now discover & isolate hijacked repeaters)

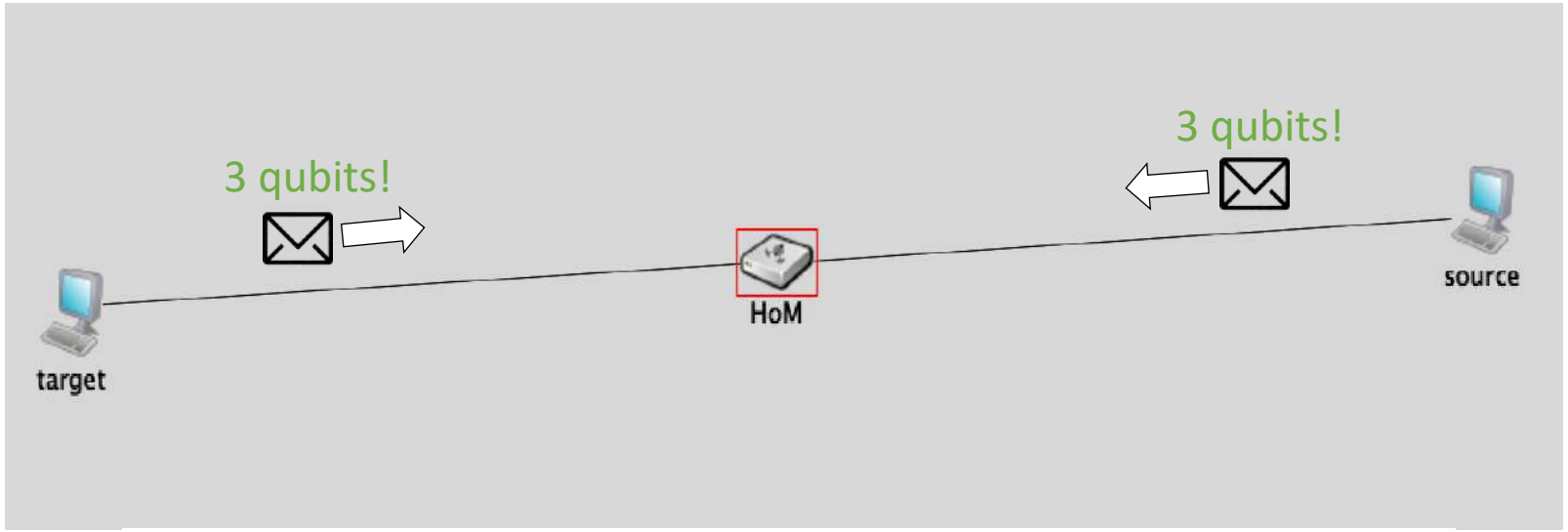
Limitation:

- Collateral damage of the approach
  - Adversary can now frame innocent repeaters & isolate them from the network

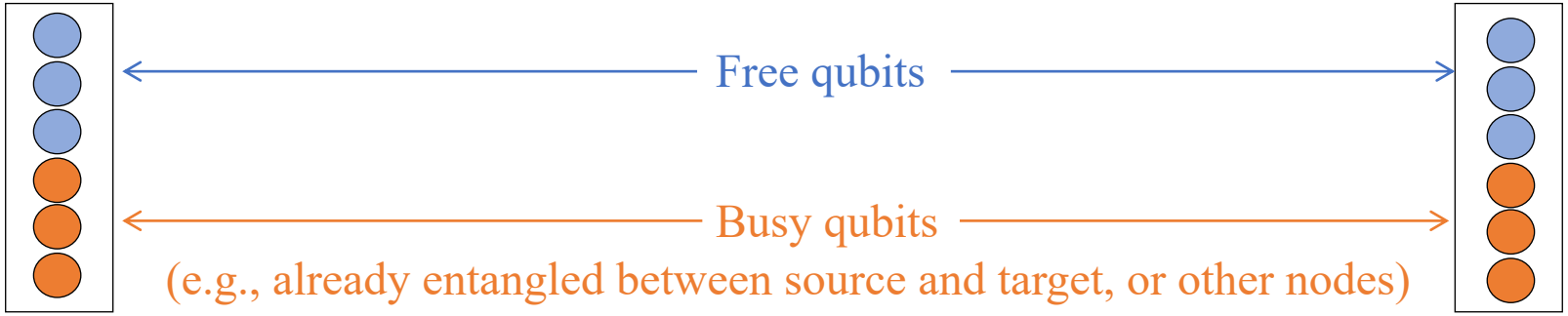
- Authors don't quantify cost of the attack
- Instead of detecting hijacked repeaters & isolate them, why don't they quantify first the attack costs, to evaluate the attack likelihood?
  - E.g., quantify costs in terms of entanglement resources & see if the attack is affordable for the adversary

  - If so, can we reduce the likelihood by adding Nick's ideas?
    - Comparison table (tomography process papers 1,2,3,4)

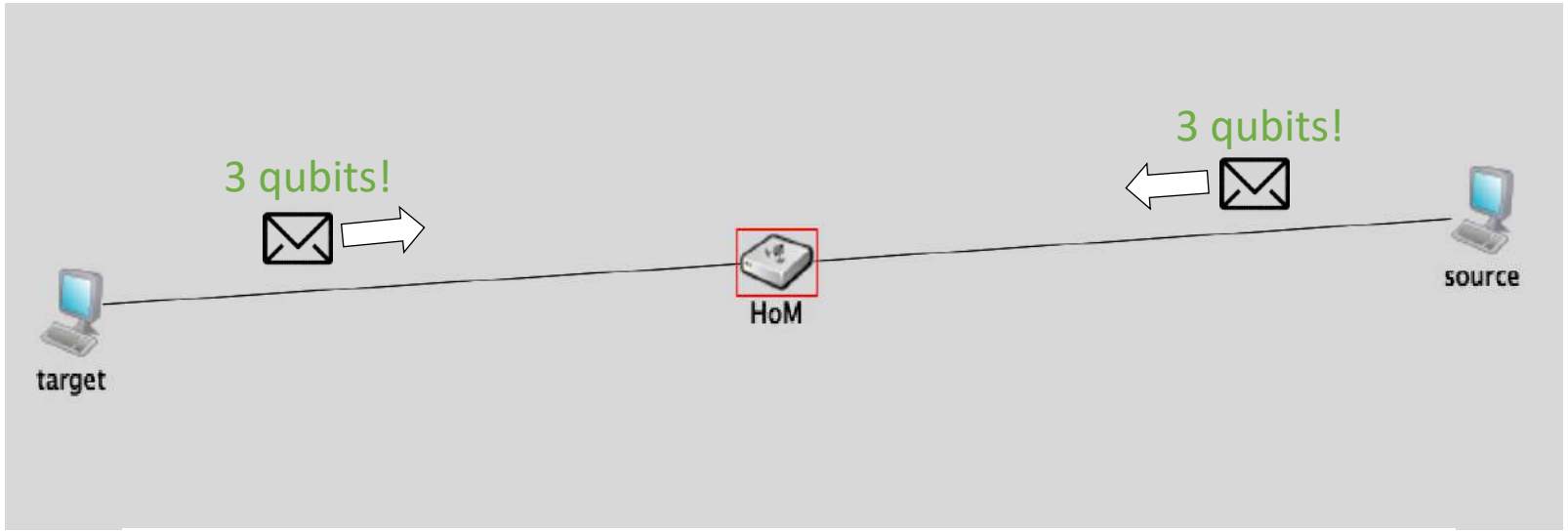
Quantify attack cost in terms of entanglement resources?



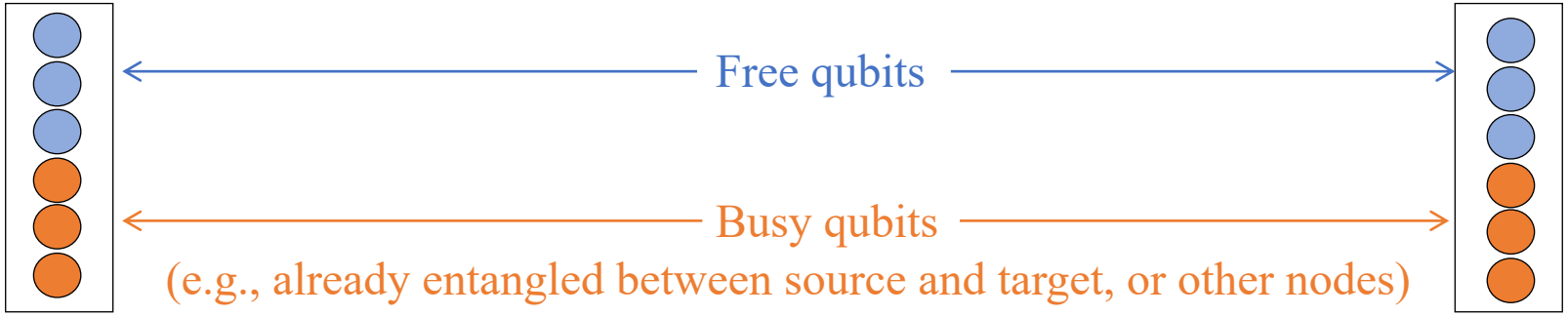
1. Repeater asks to source and target
2. Source and target return no. of qubits they want to entangle, no. of free qubits, no. of busy qubits, ...

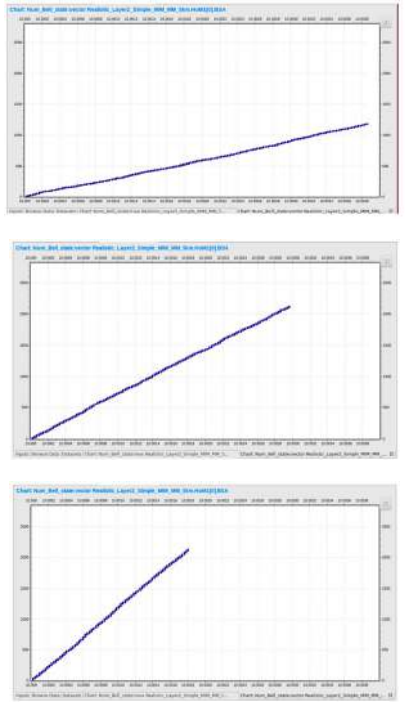


Quantify attack cost in terms of entanglement resources?



1. Repeater asks to source and target
2. Source and target return no. of qubits they want to entangle, no. of free qubits, no. of busy qubits, ...



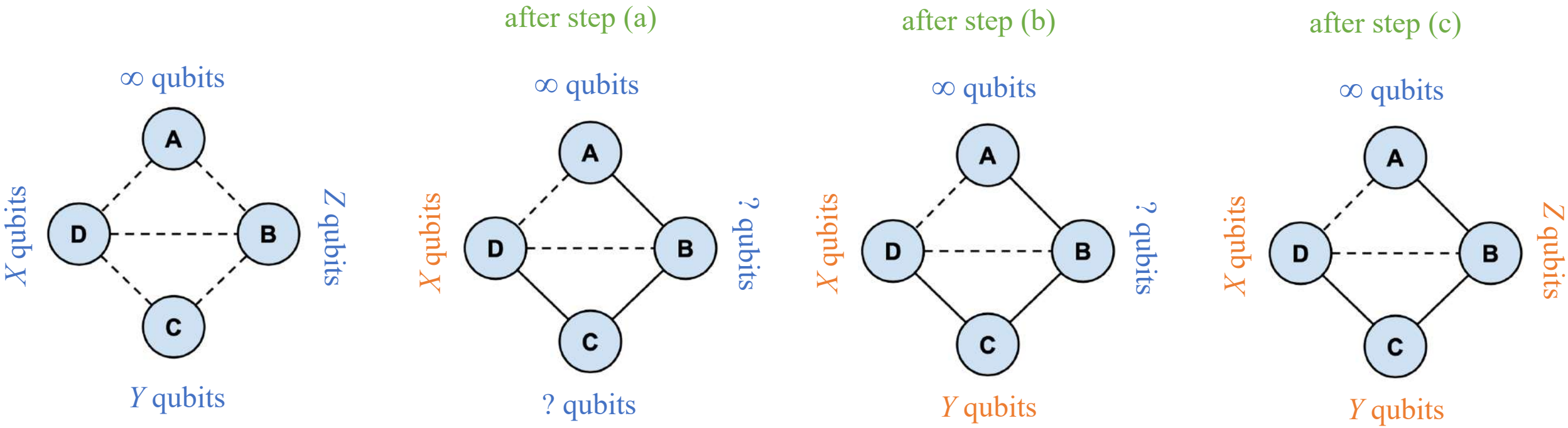


Right now, it looks like the attack is already unaffordable in terms of entanglement resources (e.g., attacker would need more than 10000 qubits to take down the whole network, or to hijack all the repeaters of the network)

Can we uncover vulnerabilities in the system of paper no. 1, so that the attack has a real impact (i.e., it gets affordable)?

- By affordable, we mean that the level of resources used by the adversary is much lower than the level of attacked resources
- Examples:
  a) Multi-hop entanglement swapping? (each qubit of the adversary affects the n qubits of a path of length n, where $n > 1$)
  b) Multi-hop entanglement swapping including loops? (same than (a), but affecting $m \cdot n$ qubits, m representing the loop)
  c) Extending short paths into long paths due to congestion?

Toy example: hijacked repeater & exhaustion of resources



Goal: the adversary (node A) wants to block all the available resources of nodes B, C and D

- Why? - E.g., to obtain a dominant position in the network?
- Make the victims unable to operate as repeaters for a given period (e.g., some minutes)?

Steps: the adversary succeeds to consume all the resources of nodes B, C and D in three steps

(a) $Path_1$: A,B,C,D (b) $Path_2$: A,B,C (c) $Path_3$: A,B

Quantifying the attack using an **effort ratio** metric?

$$\textbf{AER} = \frac{\text{no. of qubits needed to perform the attack}}{\text{no. of busy qubits in the network after performing the attack}}$$

AER (Attack Effort Ratio) represents the resources needed to perform the attack (i.e., entanglement resources of the adversary) vs. the number of resources affected by the attack (i.e., total number of busy qubits in the network)

Adding **time** to the analysis ...

In addition to computing the **effort ratio**, we could also consider

> $\Delta(t)$ **function**: e.g., time-based decreasing function that measures resource exhaustion w.r.t. amount of time since the attack was perpetrated

The attack is unaffordable if:
- AER = 1 (i.e., a kind of brute-force attack)
- $\Delta(t_0)$ = network affected, but $\Delta(t_1)$ = network unaffected (e.g., classical comms. to unlock the resources)

We can also use the following function:

- Total Exhaustion Time (TET) = $\sum_{b=0}^{\infty} \Delta(t)$

and evaluate cases in which the attack is realistic by

- Minimizing the AER
- Maximizing TET

We can conduct the experimental results by combining Quisp + Matlab + Python