Become Invisible
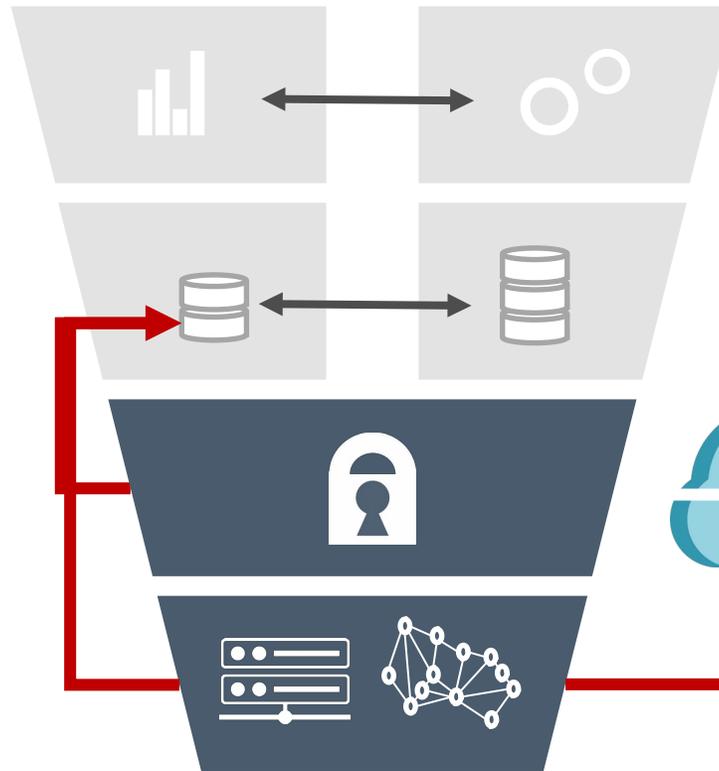
Snowpack makes you invisible to network attacks

Trust-based,
Visible Systems

Backdoors	Can be hacked	Vulnera-bilities

Infra can access data: one breach in infra is enough to compromise data!

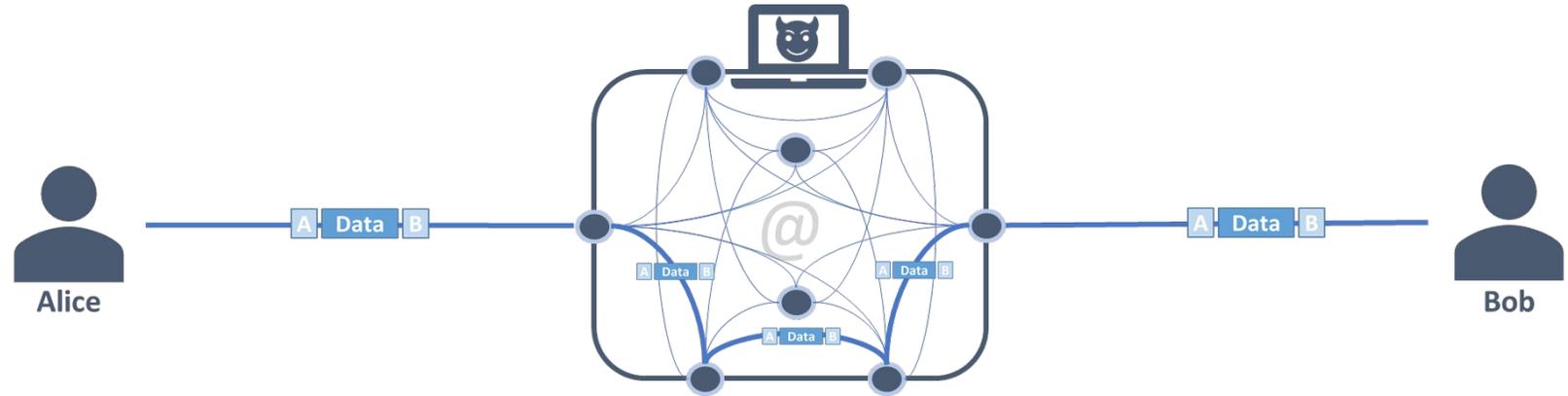Invisible,
Secured by
Snowpack

?

Hackers can't see data

With Snowpack, breaches on infra (incl. security layers & even Snowpack) leave data safe

# Invisibility: Impossible to distinguish valuable data from noise

WITHOUT Snowpack

Hackers can use IP metadata to hack and track users' data

Internet using IP addresses

Alice — A Data B — @ — A Data B — Bob

WITH Snowpack

1) Anonymization
2) Encryption
3) Invisibility
4) Transport
5) Delivery

Snowpack Overlay Network using Internet without IP addresses

Alice — A Data B — @ — A Data B — Bob
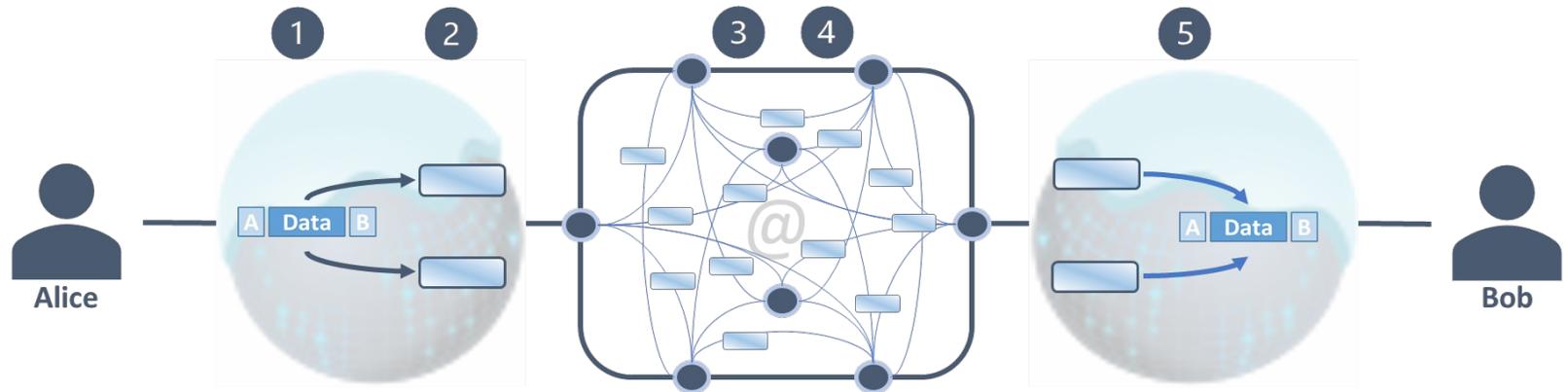
Snowpack properties

Principle
None of the materials used for the communication should have access to all the key elements of a communication: {Sender, Recipient, Content}
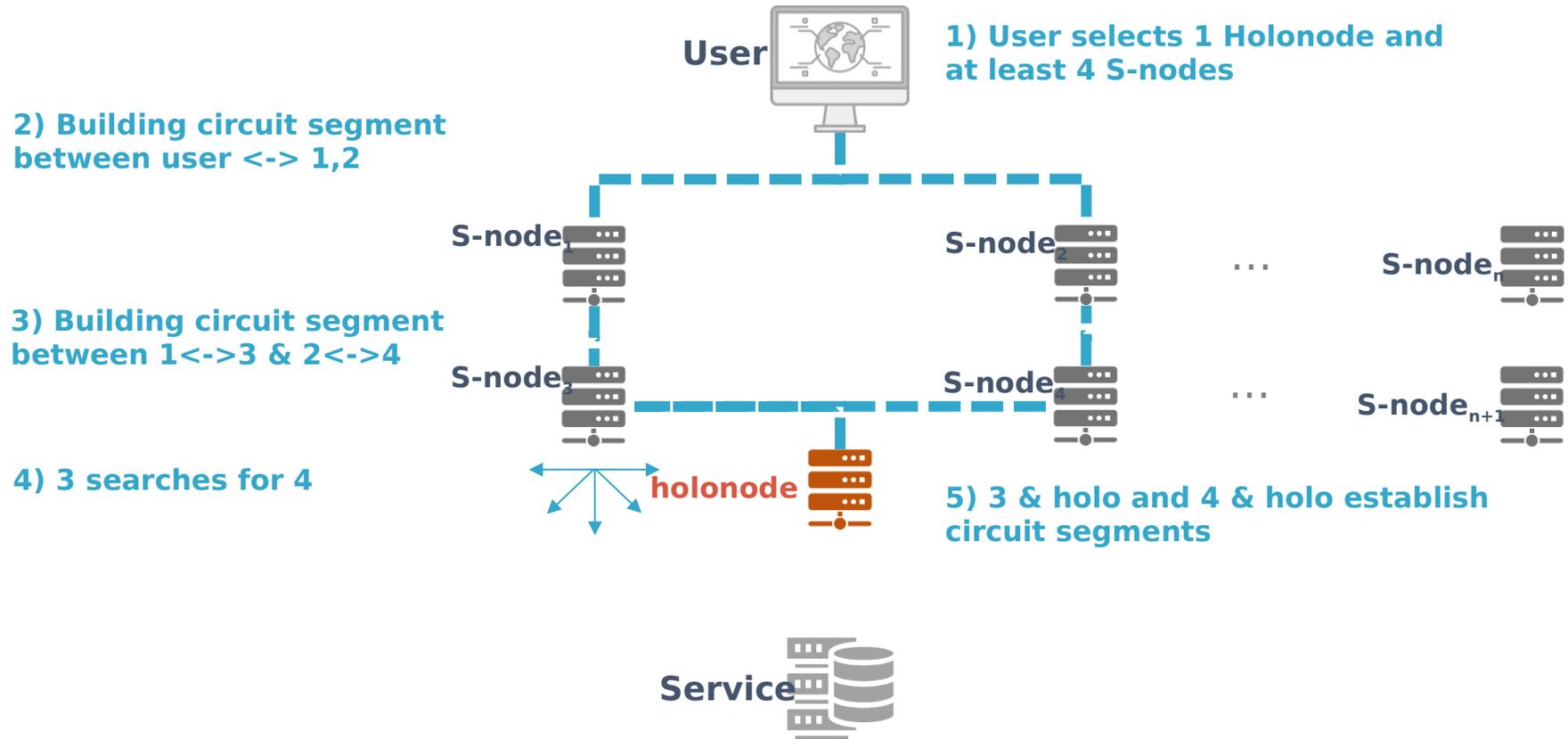
Snowpack

Privacy Mode

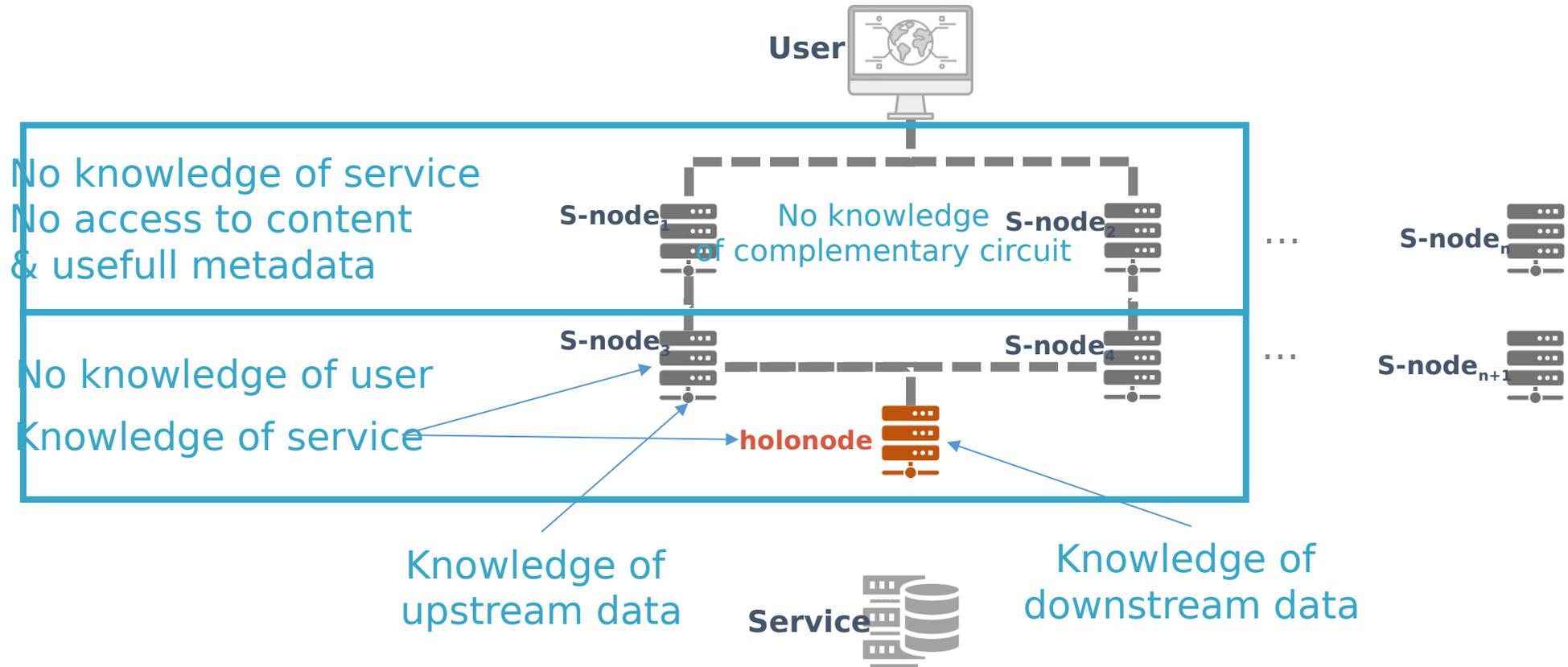Security Mode

Snowpack main protocol principles – Privacy Usage Step 1: building route

User

1) User selects 1 Holonode and at least 4 S-nodes

2) Building circuit segment between user <-> 1,2

S-node$_1$

S-node$_2$

... S-node$_n$

3) Building circuit segment between 1<->3 & 2<->4

S-node$_3$

S-node$_4$

... S-node$_{n+1}$

4) 3 searches for 4

holonode

5) 3 & holo and 4 & holo establish circuit segments

Service

Snowpack main protocol principles – Privacy Usage Summary of privacy properties

User

No knowledge of service
No access to content
& usefull metadata

No knowledge
of complementary circuit

S-node$_1$ S-node$_2$ ...   S-node$_n$

No knowledge of user

Knowledge of service

S-node$_3$ S-node$_4$ ...   S-node$_{n+1}$

holonode

Knowledge of
upstream data

Service

Knowledge of
downstream data

Usage

Easy-to-manage Snowpack application (1/4)

Easy-to-manage Snowpack application (2/4)

Easy-to-manage Snowpack application (3/4)

Easy-to-manage Snowpack application (4/4)

Internship / Phd objectives

Dynamic evaluation and control of privacy and anonymity levels of anonymization and security networks

1. Initial state-of-the-art [T0 → T0 + 9]. Analysis of publications related to the objectives of the thesis, development of a methodology for comparing anonymity and communication protection solutions.

2. Modeling and proof of the Snowpack solution [T0 + 4 → T0 + 22]. Algorithmic modeling, and mathematical proof of guarantees in the presence of various standard adversaries in the literature.

3. Quantitative analysis of anonymity and exchange protection solutions [T0 + 10 → T0 + 31]. Set up an experimental environment for testing anonymity and exchange protection solutions. Experimental campaign. Determination of solution parameters to optimize guarantees and/or efficiency.

4. Writing of thesis manuscript [T0 + 31 → T0 + 36]

Dynamic evaluation and control of privacy and anonymity levels of anonymization and security networks

1. Initial state of the art around competitors and threats models

2. Definition of attack threats models

3. Algorithmic modeling of Snowpack

    → Pursuing a CIFRE Phd with Snowpack and Sorbonne University ideally

Baptiste Polvé
Co-founder & CTO
baptiste.polve@snowpack.eu

https://snowpack.eu

Appendix

Internship - Sorbonne 2021

Users may become elements of Snowpack's infrastructure to increase their privacy

Backbone

Edge

Snowpack fragments are not anonymous

Snowpack fragments are anonymous and buried in the « noise »
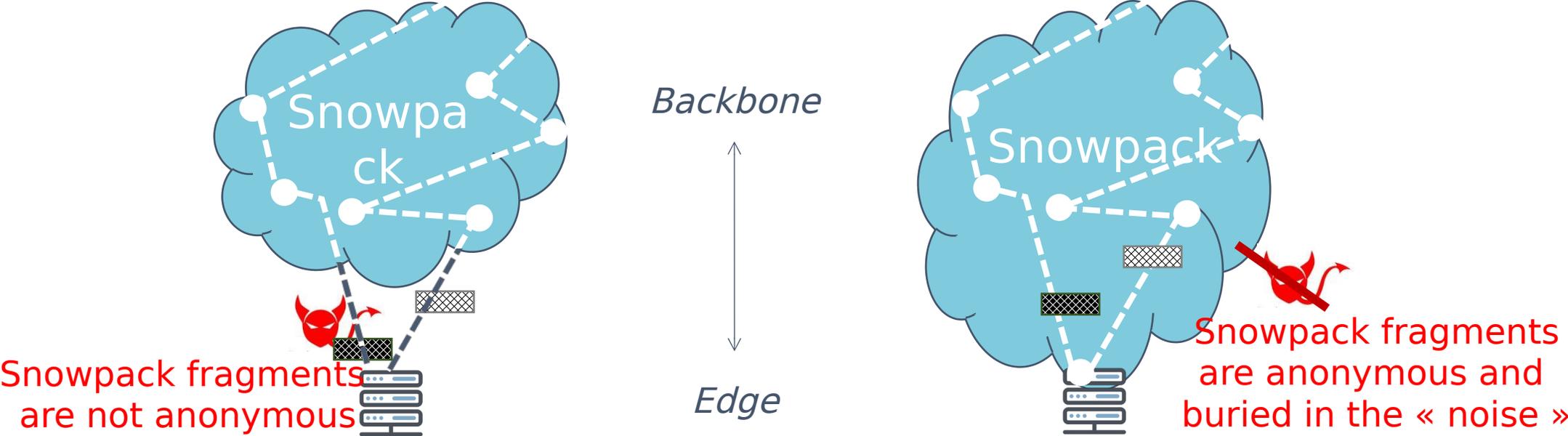
Crypto layers (Privacy mode)

packet

Layer 3

Layer 2 (incl. seq nb)

fragment

User

Layer 1: TLS

PKI
Used for:
Layer 1
Layer 2

S-node$_1$
S-node$_3$

S-node$_2$
S-node$_4$

. . . **S-node$_n$**

. . . **S-node$_{n+1}$**

holonode

Symetric Key$_{user->Master}$ is sent
through secret-sharing

Service
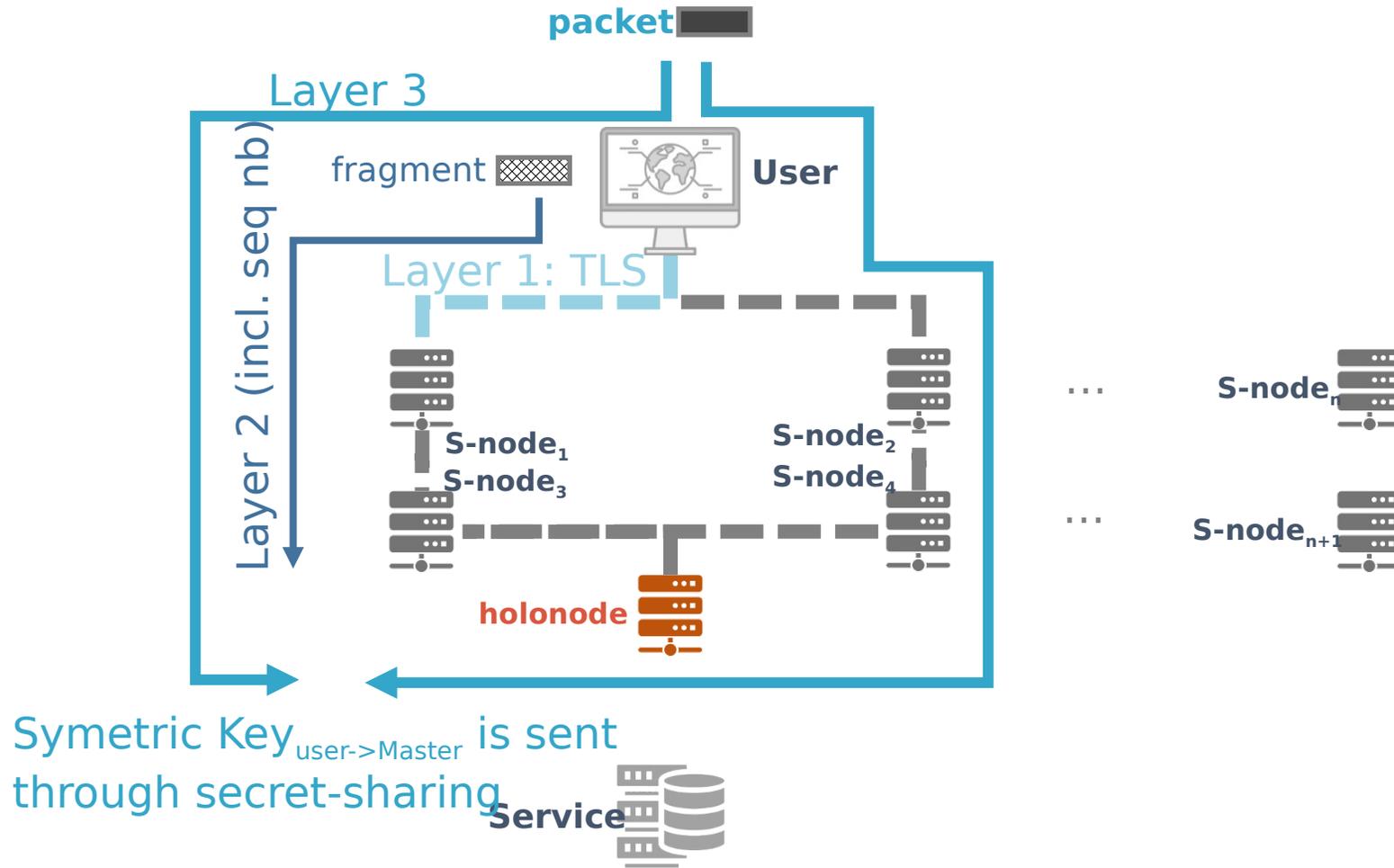
Crypto layers (Security mode)

packet

Layer 3

fragment

End point 1

Layer 1: TLS

Layer 2 (incl. seq nb)

S-node_1

S-node_2

S-node_3

S-node_4

$\cdots$ S-node_n

$\cdots$ S-node_{n+1}

PKI

Used for:
Layer 1
Layer 2

End point 2

Symetric Key$_{user->Master}$ is sent through secret-sharing
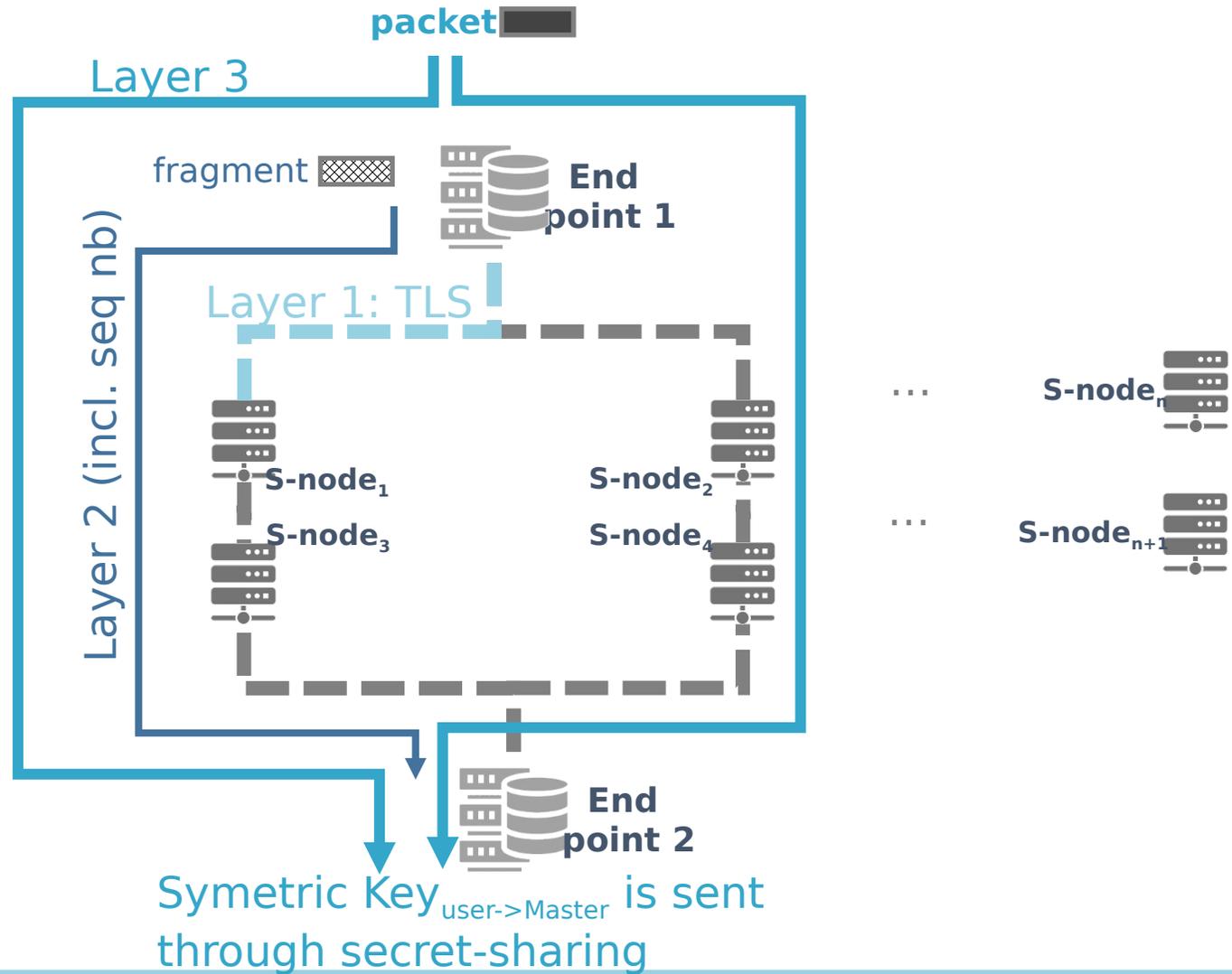
Snowpack main protocol principles - Security usage

End point 1

1) **Building circuit segments between EP1<->1,2 & EP2<->3,4**

2) **1 & 2 search for 3 & 4**

3) **Connexions 1<->3 & 2<->4**

S-node$_1$

S-node$_2$

S-node$_3$

S-node$_4$

S-node$_n$

S-node$_{n+1}$

. . .

. . .

End point 2
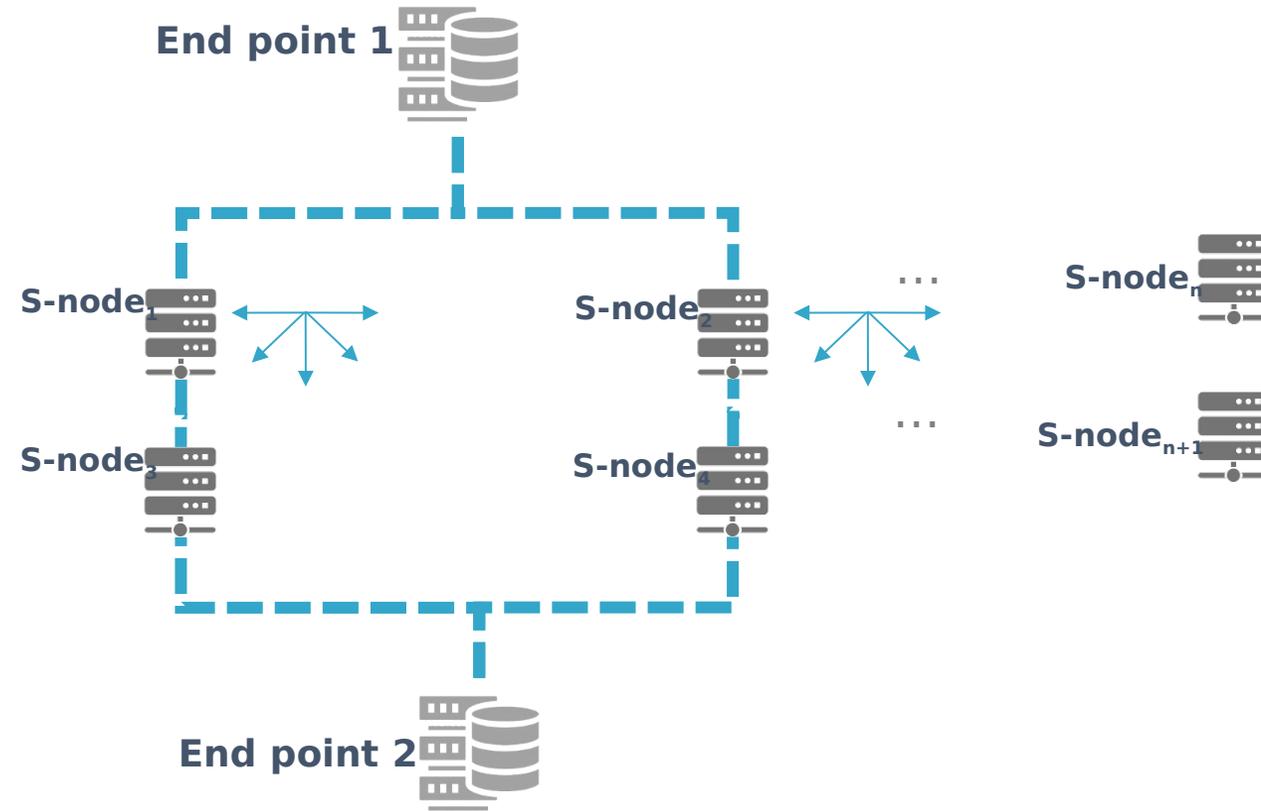
Snowpack properties

Principle
No element used for the communication should have access to all the key elements of a communication: {Sender, Recipient, Content}

Privacy:
Much harder attack through traffic analysis
No potentially vulnerable trusted-third party
Possibility to hide communication from Edge

Snowpack

Security:
3 encryption levels
No MITM
Obfuscated attack surface
Network Security outpost

Additional features from central & distributed supervision:
Capacity to guarantee Privacy & Security levels
Capacity for users to modulate these levels
Capacity to challenge nodes code from central & user level