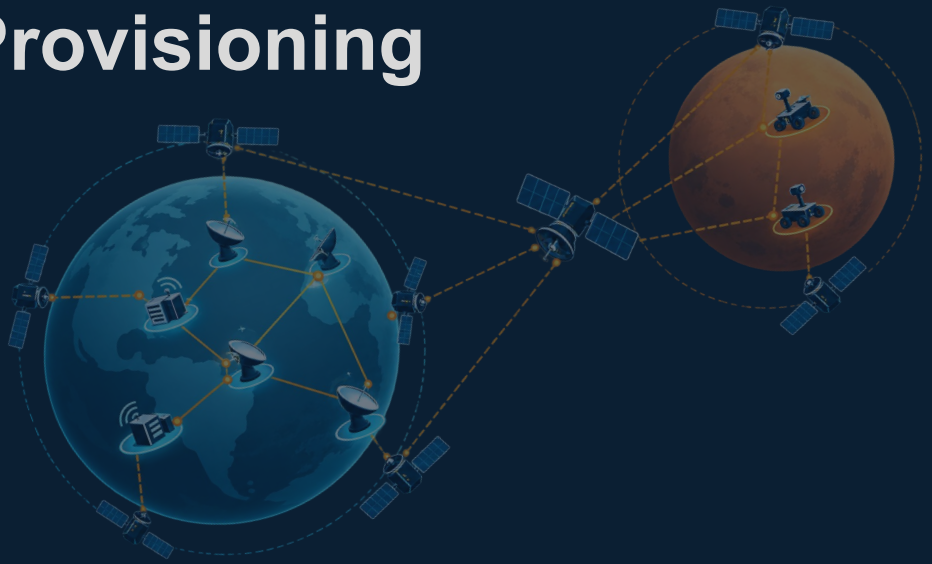
IEEE WiSEE 2026

Security-Aware Route Selection in DTNs
Towards Optimal Key Provisioning

Ramiro Detke, Pablo G. Madoery, Renato Cherini
Juan A. Fraire, Jorge M. Finochietto



unc FCEFyN CONICET

Secure communication needs routes and keys

DELAY-TOLERANT NETWORK (DTN)
Store, carry, and forward through scheduled contacts

BUNDLE PROTOCOL SECURITY (BPsec)
Integrity and confidentiality
Key management: the operator

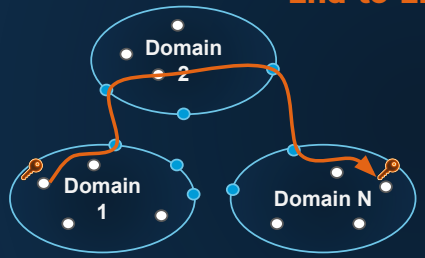
Which key scopes must be provisioned to meet a connectivity target?

Key scope
A key-sharing relationship between nodes or groups

Connectivity target
Fraction of ordered source-destination pairs with at least one usable route

Four security schemes

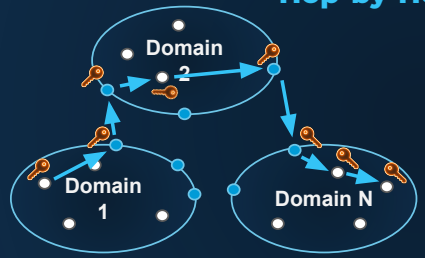
End-to-End (E2E)



Protection Span
Source to Destination

Data-at-Rest Exposure
Zero

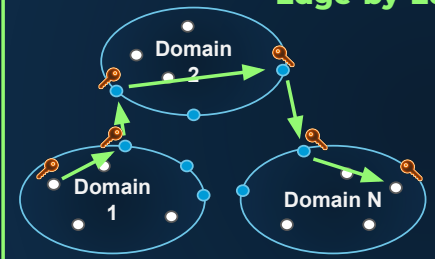
Hop-by-Hop (HbH)



Protection Span
Adjacent topological links

Data-at-Rest Exposure
High

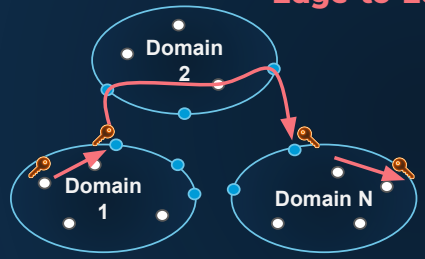
Edge-by-Edge (EbE)



Protection Span
Each domain boundary

Data-at-Rest Exposure
Medium

Edge-to-Edge (EtE)



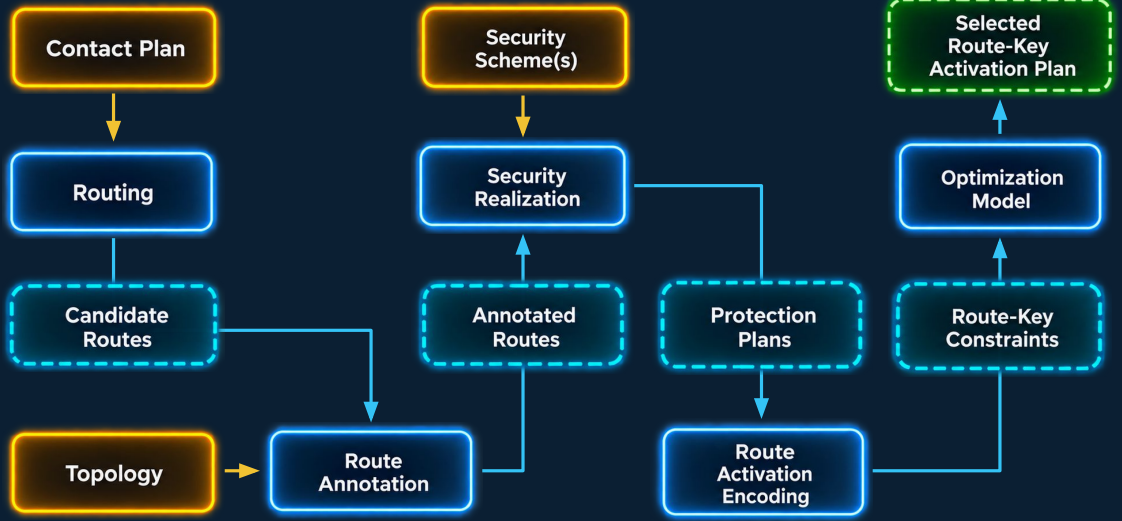
Protection Span
Boundaries of source and destination domains

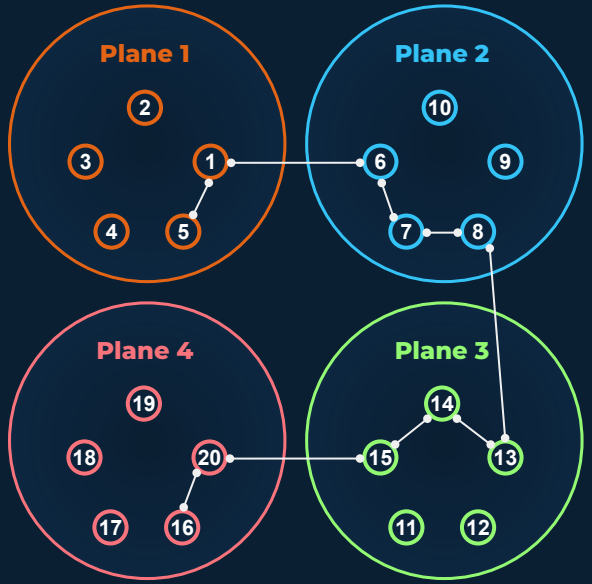
Data-at-Rest Exposure
Low

P. G. Madoery, R. Cherini, A. Cammarano, J. J. Grosso and J. M. Finochietto, "Analysis of Bundle Protocol Security Policies for Safeguarding Space Missions against Threats," 2023 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE), Aveiro, Portugal, 2023

P. G. Madoery, R. Cherini, A. Cammarano, J. Grosso and J. M. Finochietto, "Bundle Protocol Security Models and Policies for Safeguarding Space Information Networks," in *IEEE Journal of Radio Frequency Identification*, vol. 8, pp. 547-558, 2024

Routes, security schemes and keys: tightly coupled

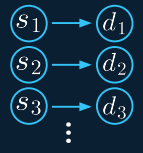




Scheme	E2E	HbH	EbE	EtE
This route	1	9	7	3
Catalog	380	62	106	112

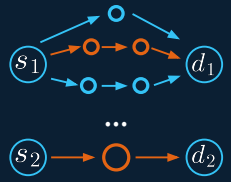
Route-aware key provisioning optimizer

1 INPUTS



D

P_{sd}

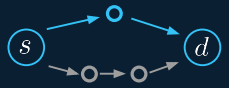


$$P = \bigcup_{(s,d)\in D} P_{sd}$$

$K(p) \subseteq K$
key scopes required by route $p \in P$

target connectivity fraction

2 DECISION VARIABLES



$$y_p = \begin{cases} 1 & \text{if route } p \text{ is activated} \\ 0 & \text{otherwise} \end{cases}$$

$$z_k = \begin{cases} 1 & \text{if key scope } k \text{ is activated} \\ 0 & \text{otherwise} \end{cases}$$

$$x_{sd} = \begin{cases} 1 & \text{if pair } (s,d) \text{ is connected} \\ 0 & \text{otherwise} \end{cases}$$

3 OBJECTIVE AND CONSTRAINTS

Objective function

$$\min \sum_{k\in K} z_k$$

Coverage target

$$\sum_{(s,d)\in D} x_{sd} \geq \lceil \gamma |D| \rceil$$

Pair-route consistency

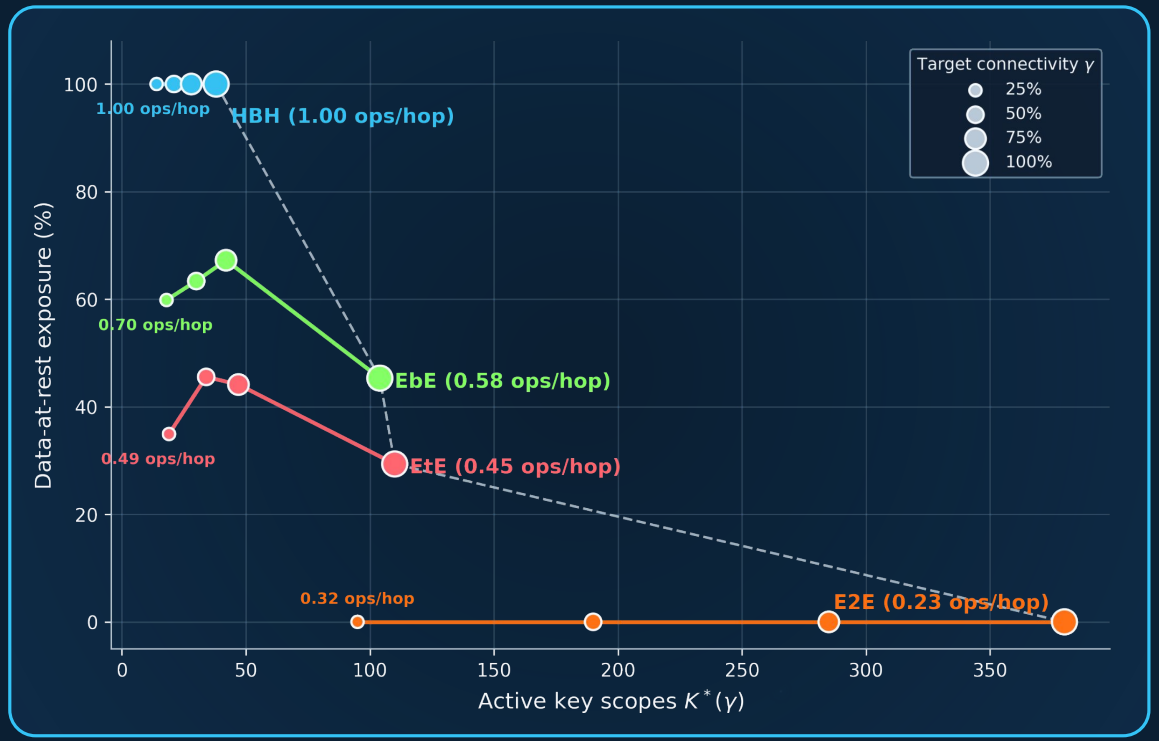
$$y_p \leq x_{sd} \qquad \forall (s,d) \in D,\ \forall p \in P_{sd}$$

$$x_{sd} \leq \sum_{p\in P_{sd}} y_p \qquad \forall (s,d) \in D$$

Route-key coupling

$$\sum_{k\in K(p)} z_k \geq |K(p)|\, y_p \qquad \forall p \in P$$

Secure connectivity has more than one cost



Four-plane scenario

20 nodes
4 domains

64 contacts
2700 s

1134 Routes

380 ordered pairs

Security policy becomes a quantitative choice

E2E · PROTECTION FIRST

Largest key set

Lowest exposure & processing

EDGE BASED · PRACTICAL MIDDLE

EtE: slightly more scopes

Lower exposure & fewer operations than EbE

HBH · KEY FOOTPRINT FIRST

Smallest active key set

Highest exposure & processing

FURTHER WORK

- Larger multi-domain scenarios
- Traffic-aware connectivity
- Hybrid per-route policies
- Key distribution scheduling

Thank you!
Questions?

Ramiro Detke
ramirof.detke@unc.edu.ar

unc FCEFyN CONICET