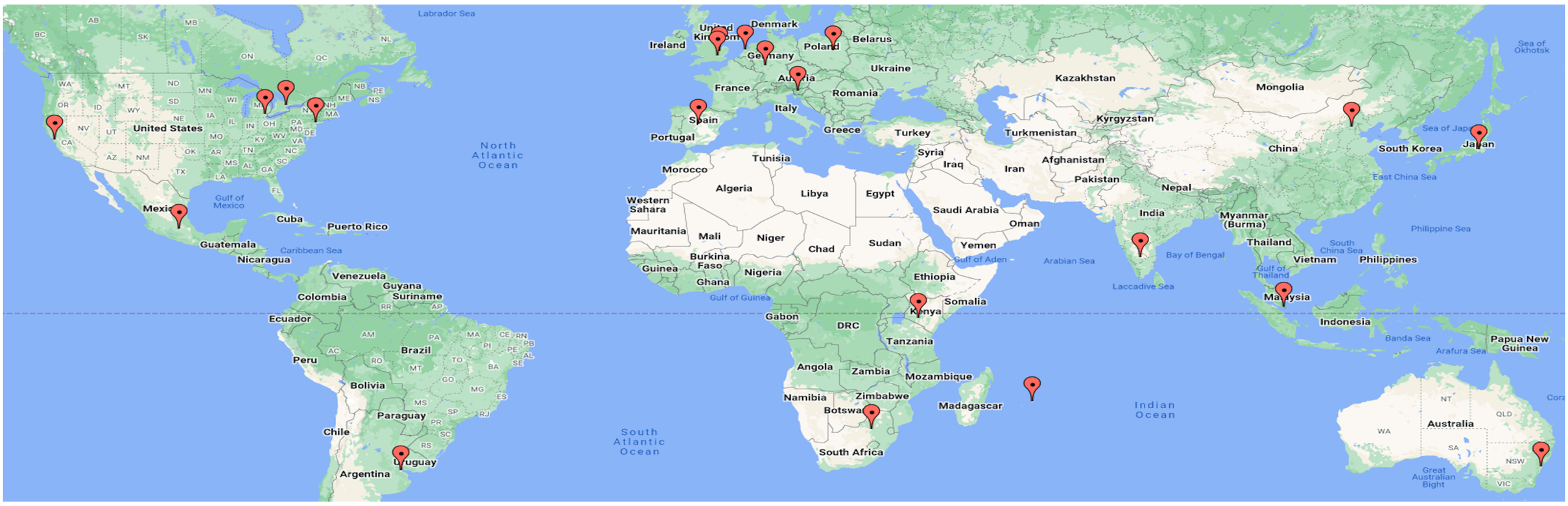
Measuring IPv6 Extension Headers Survivability with James

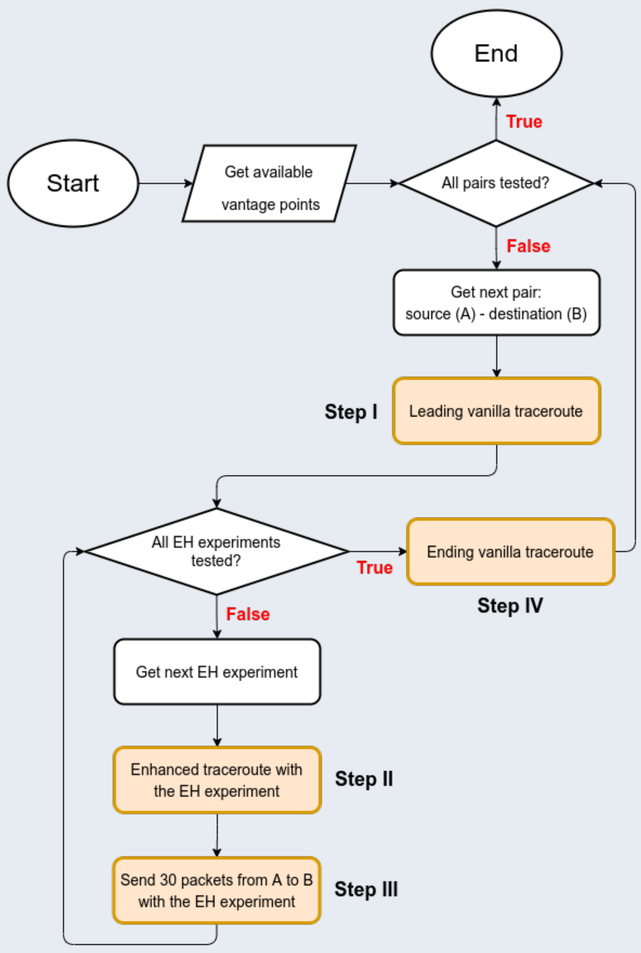
Raphaël Léas†, Justin Iurman†, Éric Vyncke*, Benoit Donnet†
† Université de Liège (Belgium), * Cisco



Research Summary

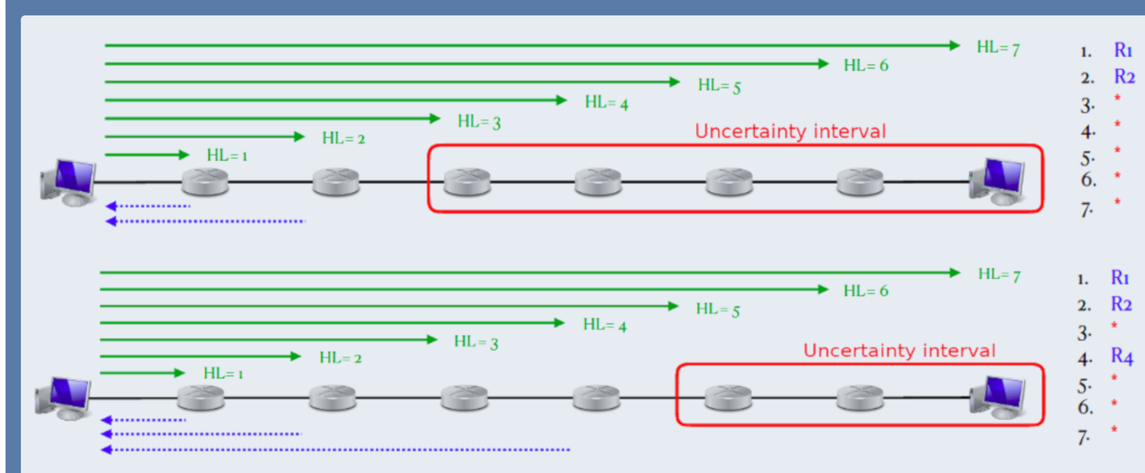
This poster introduces JAMES, a new tool for measuring how IPv6 Extension Headers (IPv6 EHs) are processed in the network. JAMES sends specially crafted Paris traceroute packets between a set of controlled vantage points. Early measurement results show that IPv6 EHs may be dropped in the network, depending on their type and the size of the Extension Header.

How it works



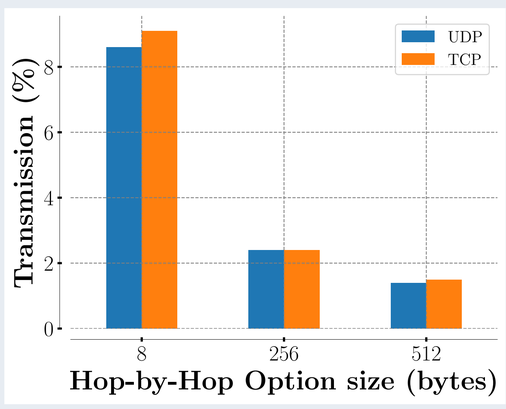
At the end of this probing phase, *pcap* data and traces that were collected are processed and transformed into user-friendly results. These results include the survivability of each Extension Header, but also transmission delays. Further analysis is applied on blocked experiments, and the guilty AS is resolved as much as possible.

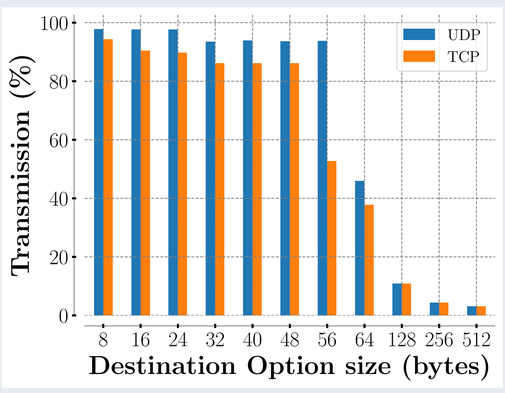
AS drop attribution



Tricky part: some routers might not respond for whatever reason (e.g., rate limiting or configured to do so). Therefore, it makes it harder to detect precisely which hop is responsible for the drop.

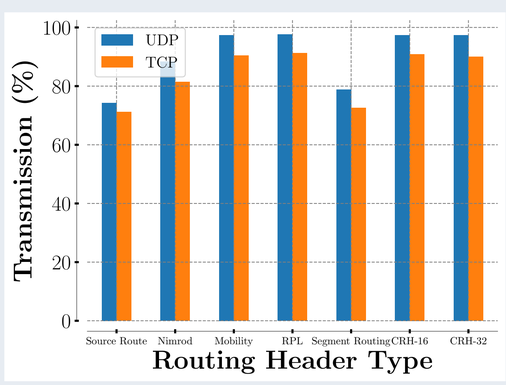
Measurements

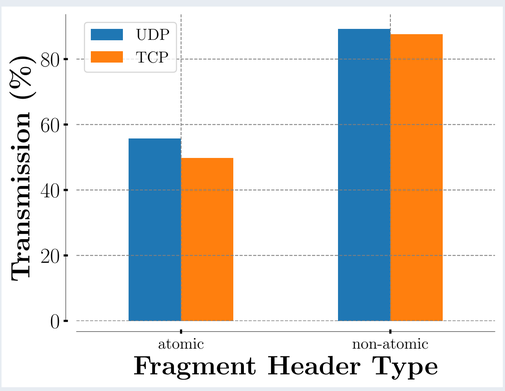




`Hop-by-Hop` Options are **not reliable** over the global Internet, even with the minimal 8-byte size where only a low 10% survive. Operators probably drop `Hop-by-Hop`'s by default for security and performance reasons, whatever the size, since there is no real use case on the "public" Internet.

`Destination` Options are **partially reliable** over the global Internet, depending on their size. In fact, they are reliable up to 32 bytes and become unreliable at 64 bytes where less than 50% survive. Possible reasons behind the difference between `UDP` and `TCP` could be (i) buffer limits for hardware lookup mechanisms, (ii) header sizes (8 bytes for `UDP` vs. 20 bytes for `TCP`), or (iii) middleboxes.





The `Routing Header` is **partially reliable**, depending on the type. However, a good practice for Routing Headers in general would be to drop by default, for obvious security reasons.

The `Fragment Header` is **unreliable** over the global Internet, although the non-atomic `Fragment Header` seems to survive more easily. The reason is probably that some stateful middleboxes drop atomic fragments because they are unexpected whenever no previous fragment with the same `Identification` number has been seen.

Note that IPSec is **reliable** over the global Internet. Indeed, the `Encapsulating Security Payload` (ESP) and the `Authentication Header` (AH) were tested too, and both survive. This would tend to demonstrate that if there is a real use case and an industry need, then a specific Extension Header is more likely to survive.

Software and datasets

JAMES is freely available along with datasets and results: `https://gitlab.uliege.be/Benoit.Donnet/james`

IETF draft

`https://datatracker.ietf.org/doc/draft-vyncke-v6ops-james/`

Acknowledgements

This work is supported by the CyberExcellence project funded by the Walloon Region, under number 2110186.

Contact

Justin Iurman – `justin.iurman@uliege.be`