Introducing privacy-preserving identifiers in LoRaWAN

Samuel Pélissier Mathieu Cunche Vincent Roca Didier Donsez

University of Lyon, INSA-Lyon, Inria, CITI - University Grenoble Alpes, Inria - University Grenoble Alpes, LIG

Context

Wireless protocols require a sort of identifier to correctly **address devices in the network**. No matter the format of such identifier (e.g.: MAC address for WiFi, or `DevAddr` for LoRaWAN), its stability in every single frame of the communication is a threat to privacy. Indeed, an attacker can then **track a device across time and space**. A counter-measure is to generate **temporary pseudonyms**; for example, Resolvable Private Addresses used in Bluetooth change every 15 minutes [3].
In this work, we investigate how **privacy-preserving identifiers** could be included in LoRaWAN, despite its **energy and computation constraints**. We describe several desirable properties of a resolvable identifier scheme. Then, we introduce several approaches to integrate random address in LoRaWAN and discuss the benefits and limitation of these solutions.

Constraints and objectives

- $\mathcal{O}_1$: Pseudonyms should be unlinkable.
- $\mathcal{O}_2$: The impact on resources consumption should be marginal.
- $\mathcal{O}_3$: The scheme should be compliant with current specifications or require only limited modifications. In particular, the general structure of the frame should remain identical.
- $\mathcal{O}_4$: An end-device should be able to change its pseudonym independently.

Re-purposing the `DevAddr` and `FCnt`

- `DevAddr`: a random identifier used during the communication.
- `FCnt`: a counter incremented for each message.

As both fields are used for tracking [4, 2], we propose to re-use the bits of the `FCnt` for our address scheme. This supposes to integrate the ordering property of the `FCnt` in the new addressing scheme.

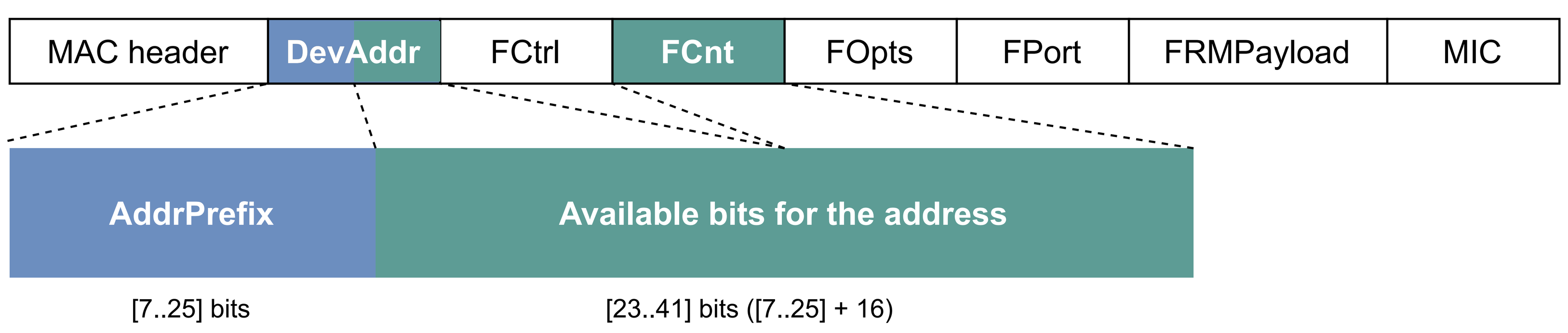
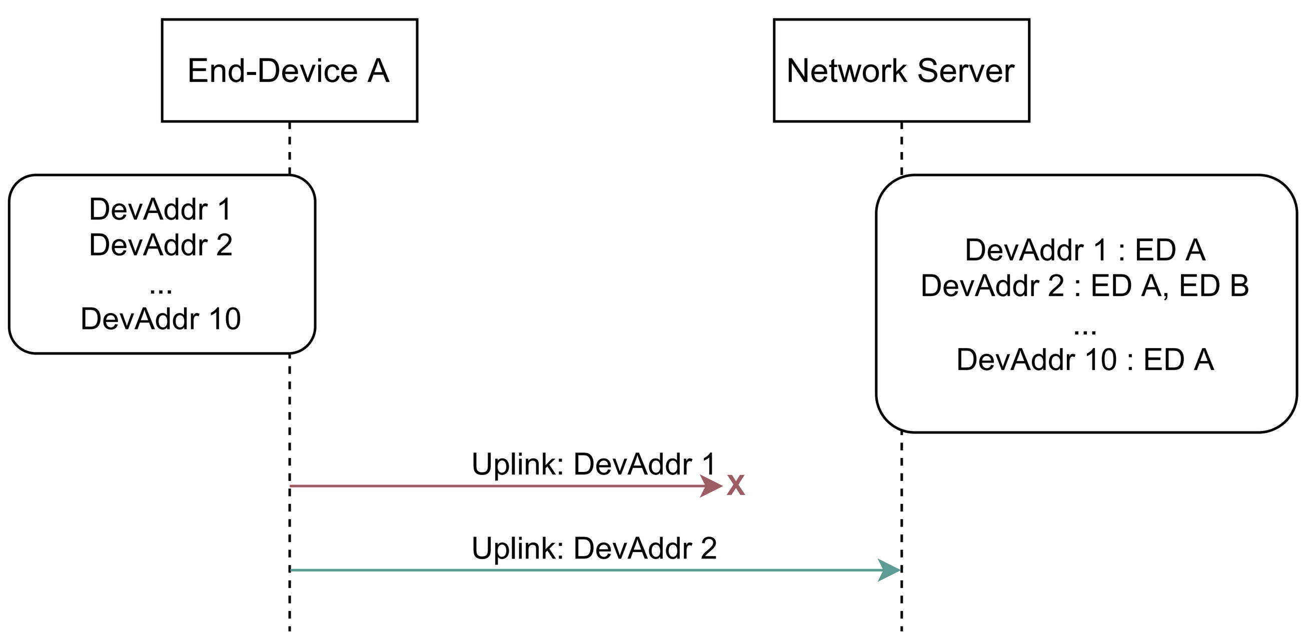


Figure 1:Structure of a LoRaWAN PHY payload, with relevant fields re-purposed for a new addressing scheme

Address generation

Adapted from SlyFi, proposed for WiFi [1].

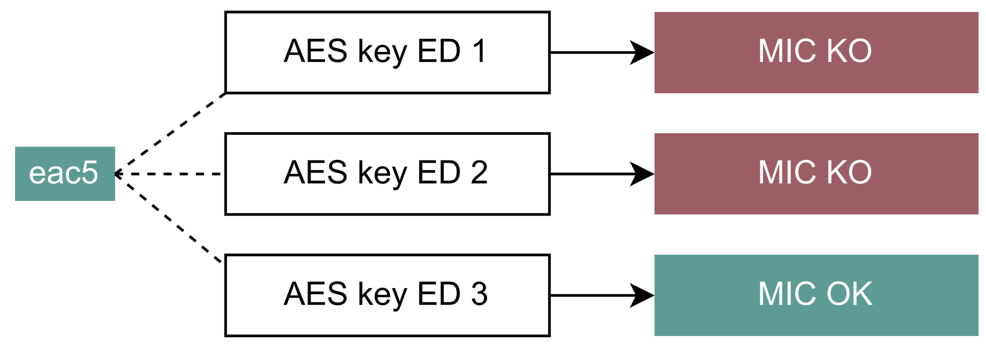
Both the End-Device and the Network Server generate a list of addresses based on a secret obtained during the Join process (e.g. the session key, `NwkSKey`).



The encrypted addresses are generated using AES-CTR by encrypting a counter (e.g.: the `FCnt`).

Address resolution

The Network Server searches the address in a hash table ($O(1)$) to find the corresponding session key(s). It then computes the MIC.



Such scheme introduces limited overhead:

- Same length of messages (same format)
- Low computation
  - 6-bytes encryption for each new address
  - Few MIC computation server-side

Renewal strategies

If only one `DevAddr` changes, does it really matter?

The best renewal strategy provides:

- Synchronisation between the End-Device and the Network Server;
- Synchronisation between the end-devices themselves;
- Randomized patterns.

The address has to be renewed for every single `uplink` message.

Conclusion

We propose a privacy-preserving addressing scheme for LoRaWAN to protect against tracking. Based on encrypted addresses and frequent independent renewals, it requires minor revisions to the specification. Our proposal introduces a limited overhead, both computation, energy, and memory-wise. A simplified proof-of-concept is currently under development.

Acknowledgements

This work has been supported by the ANR-BMBF PIVOT project (ANR-20-CYAL-0002), H2020 SPARTA project and the INSA-Lyon SPIE ICS IoT Chair.

References

[1] B. Greenstein, D. McCoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. Improving wireless privacy with an identifier-free link layer protocol. In *Proceeding of the 6th International Conference on Mobile Systems, Applications, and Services - MobiSys '08*, page 40, Breckenridge, CO, USA, 2008. ACM Press. ISBN 978-1-60558-139-2. doi: 10.1145/1378600.1378607.

[2] S. Pélissier, M. Cunche, V. Roca, and D. Donsez. Device re-identification in LoRaWAN through messages linkage. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 98–103, 2022.

[3] B. SIG. *Bluetooth Core Specification v4.0*. 2010. URL `https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=456433`. Accessed: 2019-08-30.

[4] M. Vanhoef, C. Matte, M. Cunche, L. S. Cardoso, and F. Piessens. Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '16, pages 413–424, New York, NY, USA, May 2016. Association for Computing Machinery. ISBN 978-1-4503-4233-9. doi: 10.1145/2897845.2897883.