Secure PMIPv6-based Mobility Solution for LoRaWAN

Authors:

Hassan JRADI*†, Abed Ellatif SAMHAT*, Fabienne NOUVEL†,
Mohamad MROUE*, Jean-Christophe PREVOTET†

Affiliations:

*Lebanese University — CRSI
†INSA de Rennes — IETR

Presented By:

Hassan JRADI
Hassan.Jradi@insa-rennes.fr

The Twenty-First International Conference on Networks (ICN 2022)

April 24, 2022 to April 28, 2022 - Barcelona, Spain

Hassan JRADI

- Received Bachelor of Engineering in "Telecommunications" from the Lebanese University in 2019.
- Received Master of Engineering in "Telecommunications, Network and Security" from the University Saint Joseph of Beirut in 2019.
- Currently a Ph.D. student at:
  - Lebanese University – CRSI, Lebanon
  - INSA de Rennes – IETR, France
- Research interests: Internet of Things, Low Power Wide Area Networks, Network Security and Mobility Management.

Outline

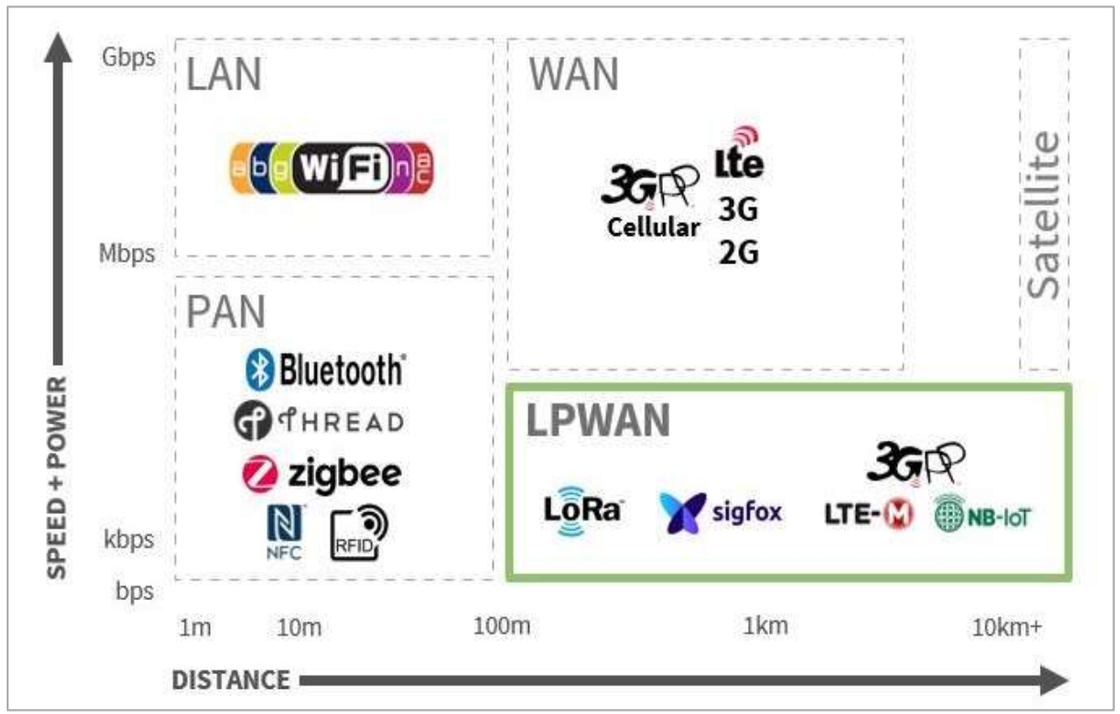
1. Introduction
2. Problematic
3. Contribution
4. Proposed Solution
5. Results & Analysis
6. Conclusion

1. Introduction

- The widespread of IoT had stimulated the invention of new communication technologies.

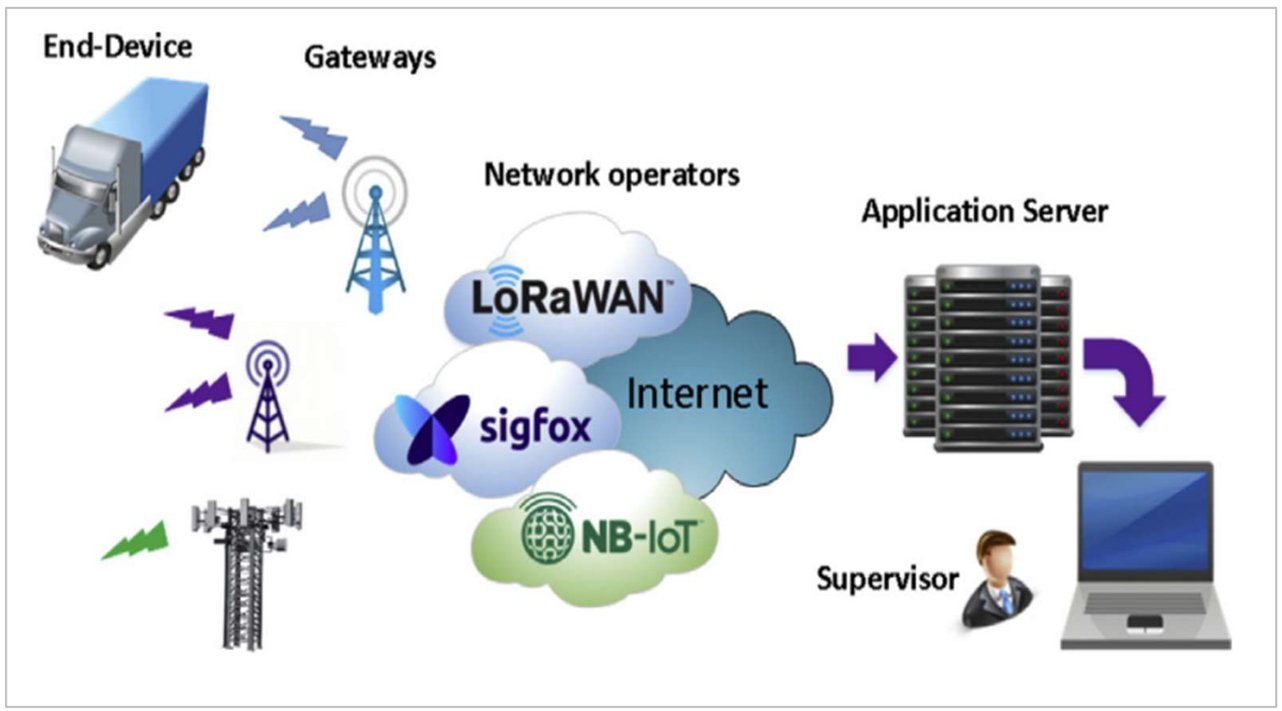
- LPWAN[1] characteristics:
  - Low power consumption
  - Long coverage range
  - Low data rate

- LoRaWAN[2]: the most important LPWAN technology.



2. Problematic (1/2)

- Several applications require secure mobility solution.
- The solution should be independent of the used technology.



2. Problematic (2/2)

- Network layer protocols like IPv4 and IPv6 supports mobility.
- PMIPv6[3] is one of IPv6 protocol extensions.
- PMIPv6 does not deploy an authentication mechanism.
- PMIPv6 is not directly compatible with LoRaWAN.

. Network Architecture . Payload Length < 255 Bytes

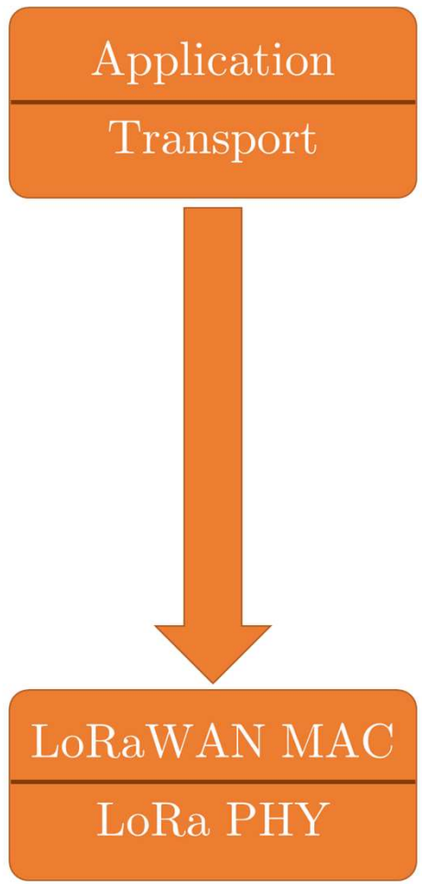
3. Contribution

1. Proposal of PMIPv6-based **mobility** solution for **LoRaWAN**.

2. Proposal of an **authentication** scheme to provide **secure access**.

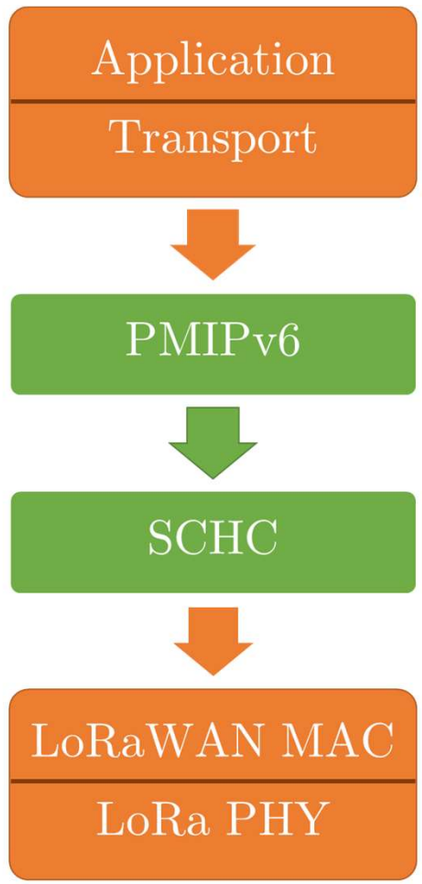
4. Proposed Solution 4.1. Protocol Stack

- Protocol stack for the communication between the mobile node and the network.
- Use of IPv6 and PMIPv6 at network layer → mobility and global addressing.
- Max LoRaWAN payload = 255 Bytes → compression needed.
- Use of SCHC[4] as an adaptation layer.



4. Proposed Solution 4.1. Protocol Stack

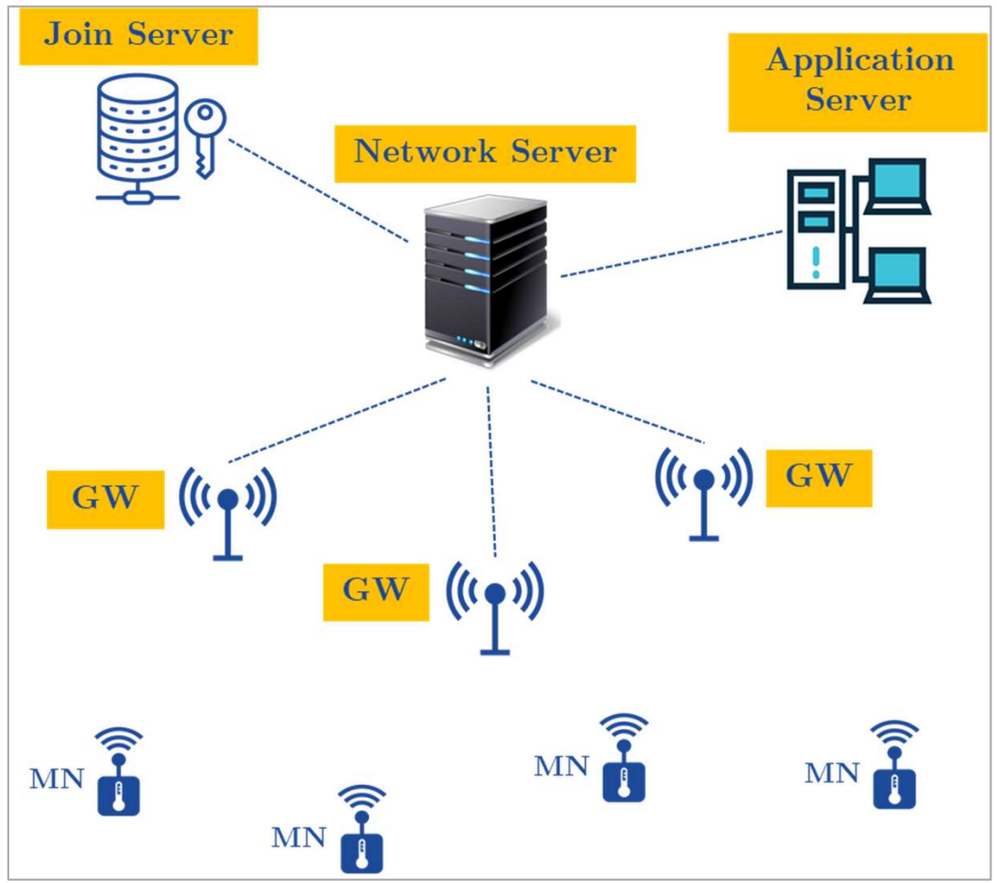
- Protocol stack for the communication between the mobile node and the network.
- Use of IPv6 and PMIPv6 at network layer → mobility and global addressing.
- Max LoRaWAN payload = 255 Bytes → compression needed.
- Use of SCHC[4] as an adaptation layer.



4. Proposed Solution 4.2. Network Architecture

- LoRaWAN network:

  .GW .NS .JS .AS



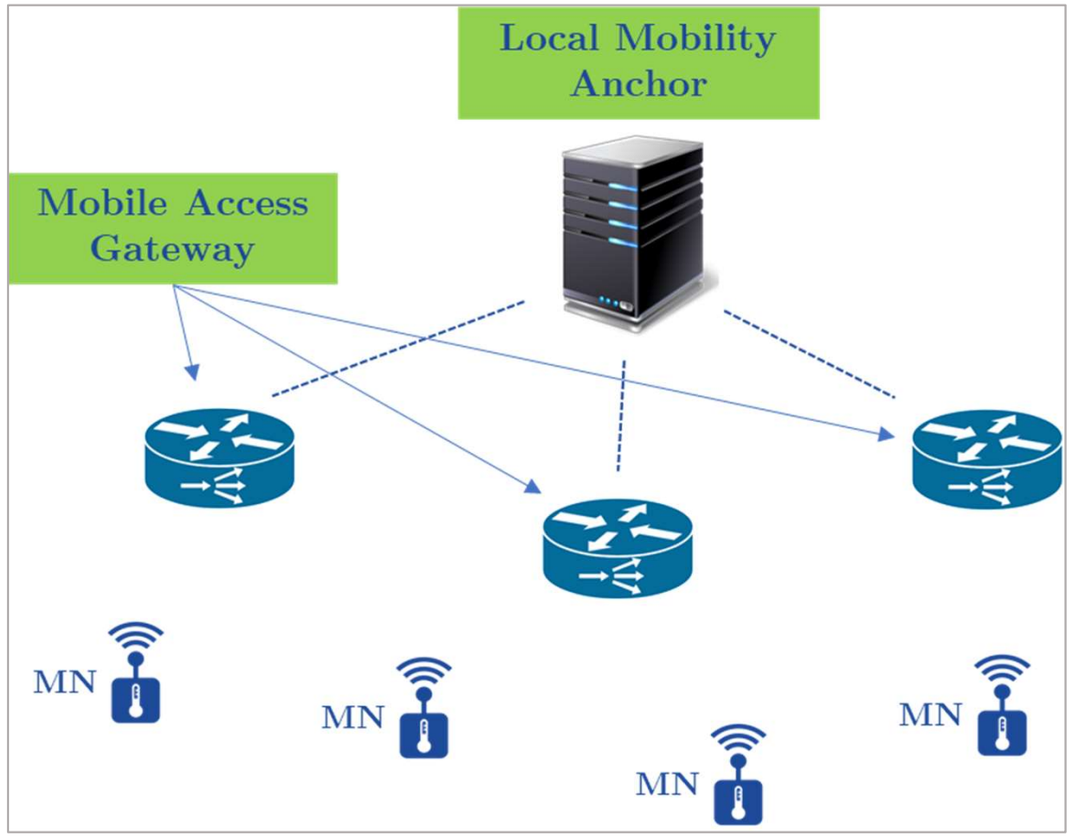
4. Proposed Solution 4.2. Network Architecture

- LoRaWAN network:

  .GW .NS .JS .AS

- PMIPv6 network:

  .MAG .LMA



4. Proposed Solution 4.2. Network Architecture

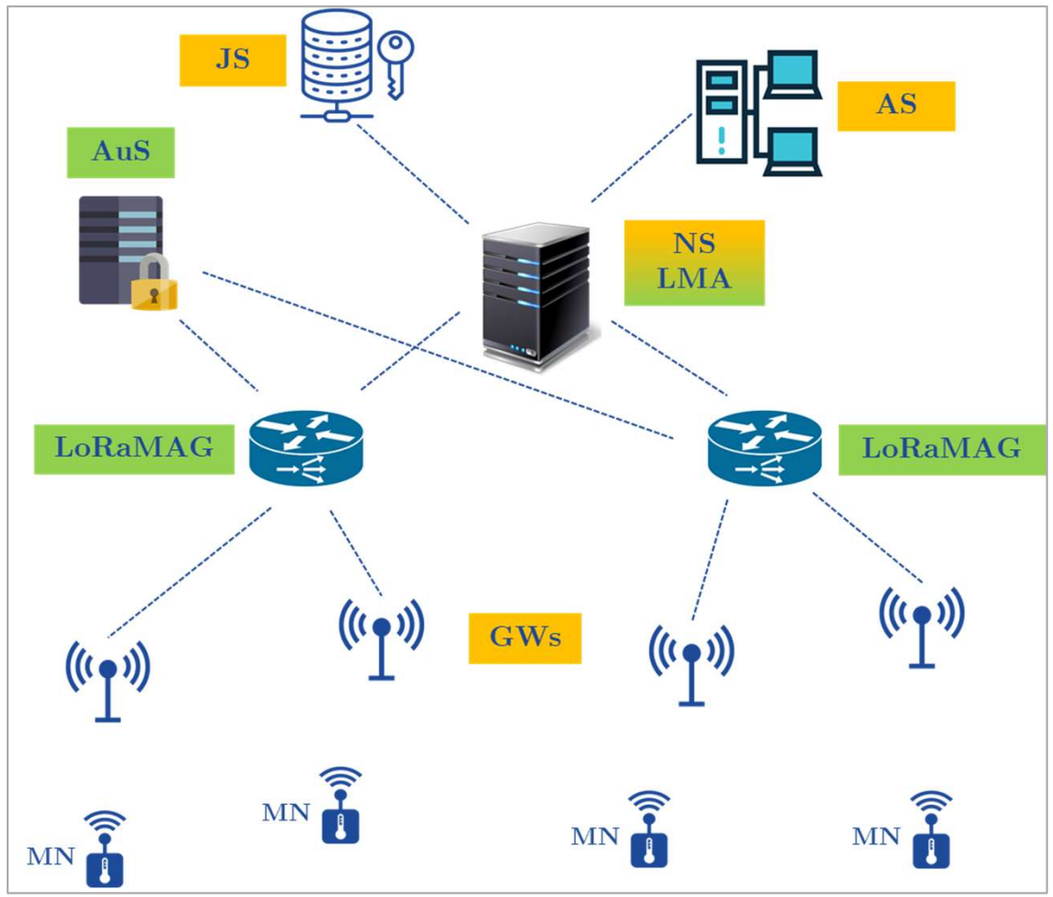
- LoRaWAN network:

  .GW .NS .JS .AS

- PMIPv6 network:

  .MAG .LMA

- How to integrate PMIPv6 in LoRaWAN ?
  - NS plays the role of LMA
  - New entities: LoRaMAG , AuS

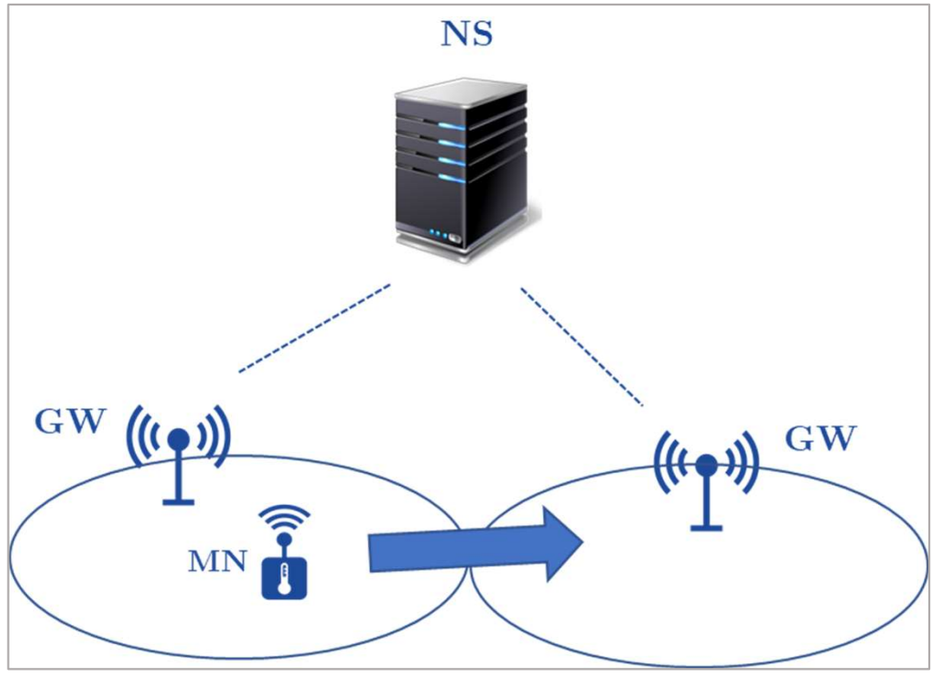


4. Proposed Solution 4.3. Authentication Scheme

- Authenticate MN with LMA and LoRaMAG.
- Two phases:
  1. Registration phase
  2. Authentication phase
- Two cases:
  1. Intra domain
  2. Inter domain

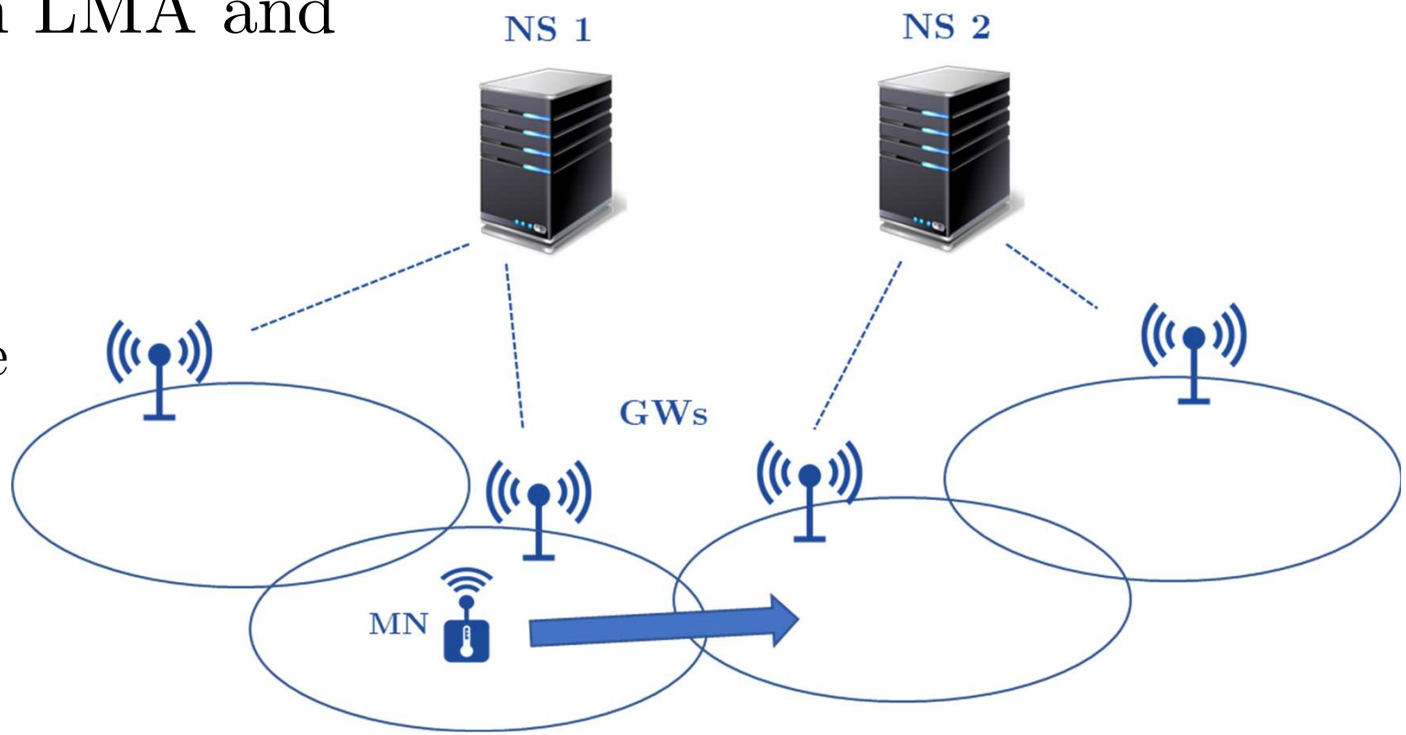
4. Proposed Solution 4.3. Authentication Scheme

- Authenticate MN with LMA and LoRaMAG.
- Two phases:
  1. Registration phase
  2. Authentication phase
- Two cases:
  1. Intra domain
  2. Inter domain



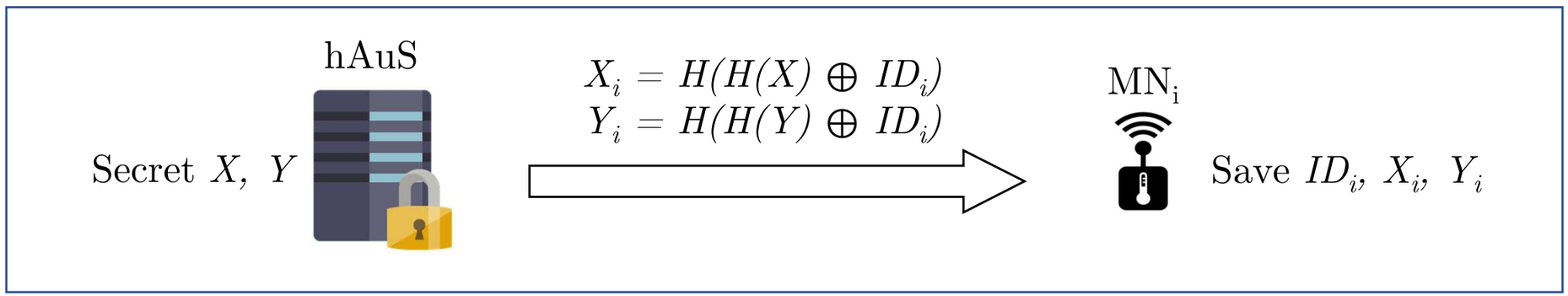
4. Proposed Solution 4.3. Authentication Scheme

- Authenticate MN with LMA and LoRaMAG.
- Two phases:
  1. Registration phase
  2. Authentication phase
- Two cases:
  1. Intra domain
  2. Inter domain



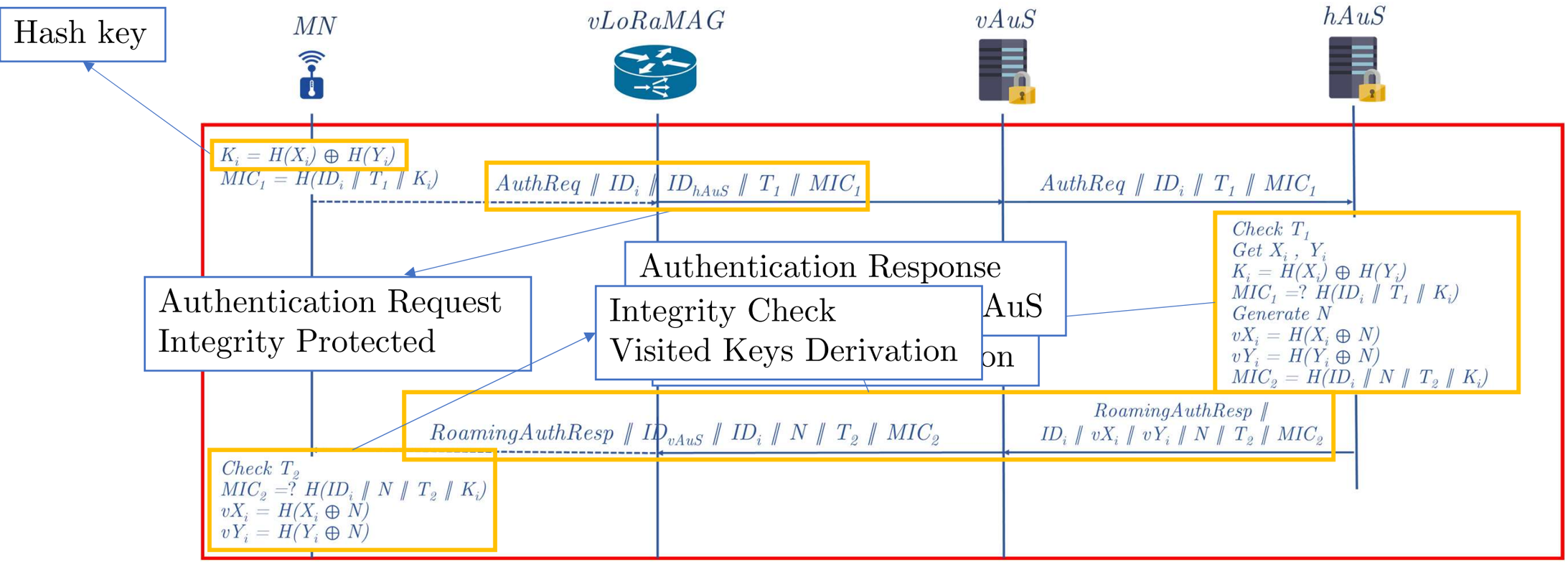
4. Proposed Solution 4.3. Authentication Scheme

- Registration Phase:

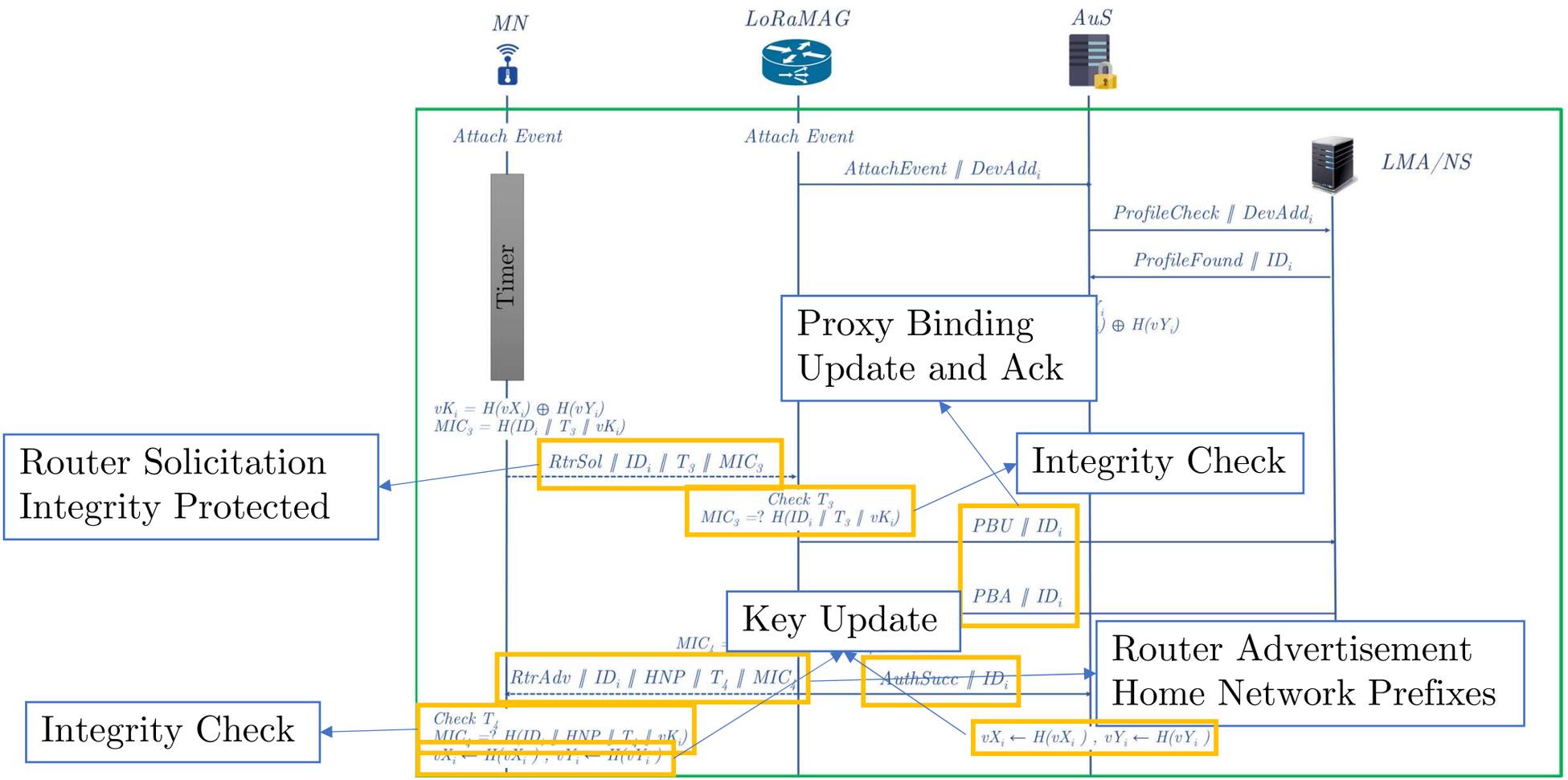


4. Proposed Solution 4.3. Authentication Scheme

- Authentication Phase: Roaming Case - Once per visited domain

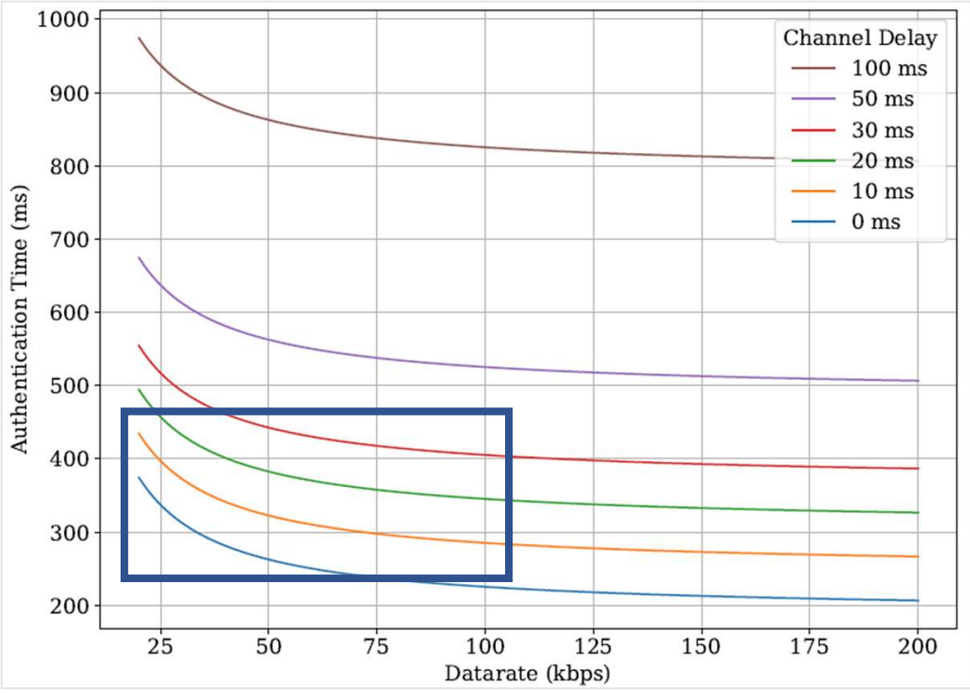


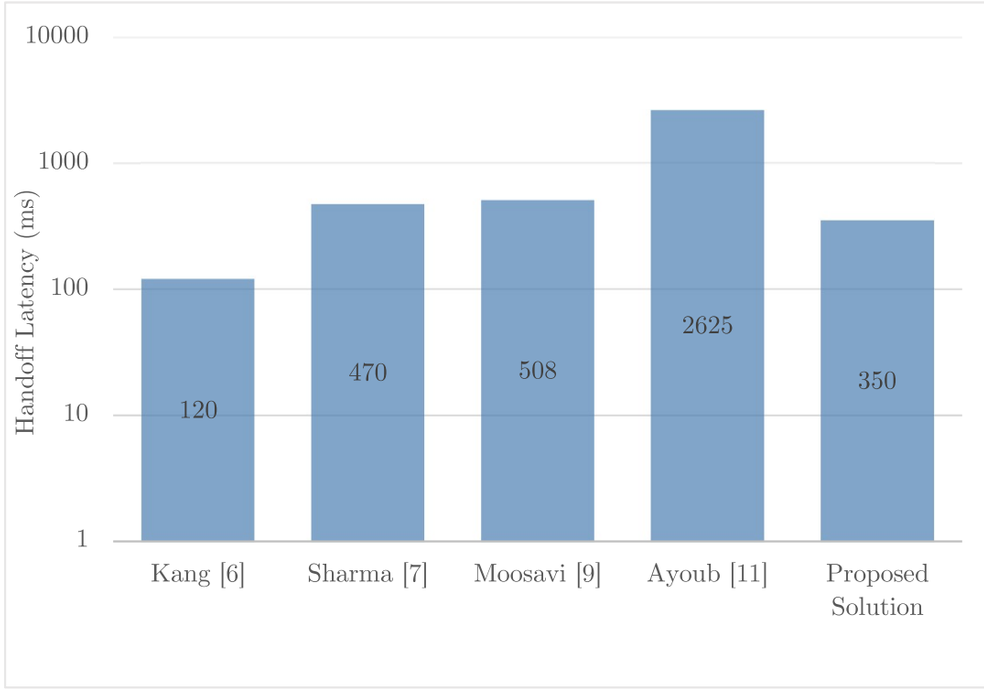
4. Proposed Solution 4.3. Authentication Scheme



5. Results & Analysis 5.1. Performance Evaluation

- Simulation using Network Simulator 3.



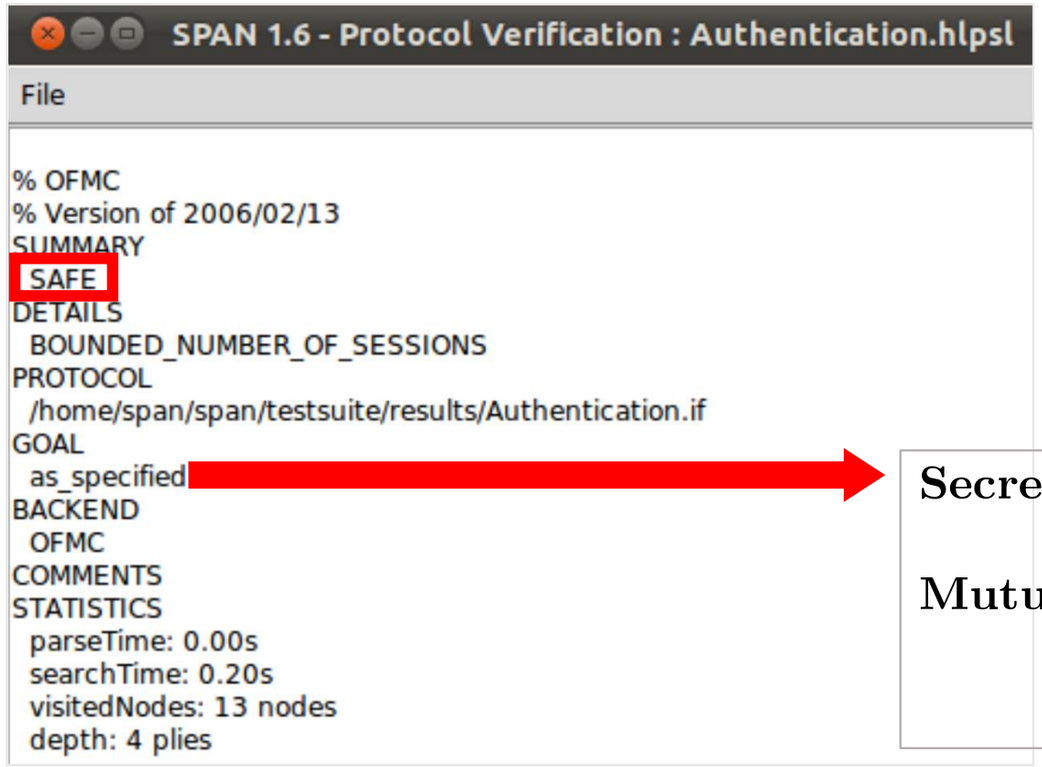


5. Results & Analysis 5.2. Security Analysis

- Device re-authentication
- Spoofing signaling message
- Address squatting and spoofing
- Old address control
- Mutual authentication
- Key freshness
- Replay attack

5. Results & Analysis 5.3. Security Validation

- AVISPA[6]: Automated Validation of Internet Security Protocols.



Secrecy of:
$\mathbf{X_i}$, $\mathbf{Y_i}$, $\mathbf{K_i}$, $\mathbf{vK_i}$, $\mathbf{vX_i}$, $\mathbf{vY_i}$
Mutual authentication:
MN and vLoRaMAG
MN and vAuS

References

1) Mekki, Kais, et al. "A comparative study of LPWAN technologies for large-scale IoT deployment." ICT express 5.1 (2019): 1-7.
2) Sornin, Nicolas, et al. "Lorawan specification." LoRa alliance 1 (2015).
3) Gundavelli, Sri, et al. "Proxy mobile ipv6." (2008).
4) Minaburo, Ana, et al. "Schc: Generic framework for static context header compression and fragmentation." RFC 8724 (2020): 1-71.
5) ns3: [Online]. nsnam.org
6) AVISPA: [Online]. people.irisa.fr/Thomas.Genet/span/

Thank You !
Q & A