Meet-up 2019 | Doctorants & Industrie

C-ITS PKI protocol: Performance evaluations in a real environment

Farah HAIDAR[1,2,3]

Arnaud KAISER[1], Brigitte LONC[2], Pascal URIEN[3]

[1]IRT SystemX, [2]Renault, [3]Télécom ParisTech

1. CONTEXT

- In the near future, vehicles will communicate by broadcasting data such as position, speed, heading, etc… in order to improve road safety and traffic efficiency.
- These data can be collected and used to track vehicles.

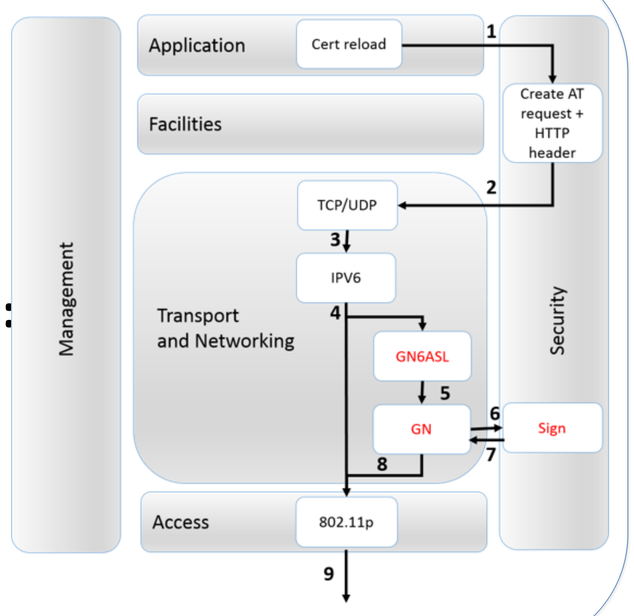
2. CHALLENGES AND MOTIVATIONS

- To cope with this privacy issues in C-ITS, Standardization bodies recommend to have 60 to 100 valid pseudonym identity (i.e Authorization Ticket or AT) per week and frequently change them to prevent tracking.
- Changing frequently means that vehicles need to reload frequently their pool of pseudonym certificates through requests sent to the PKI.
- **What about the performance of pseudonym certificates reloading?**

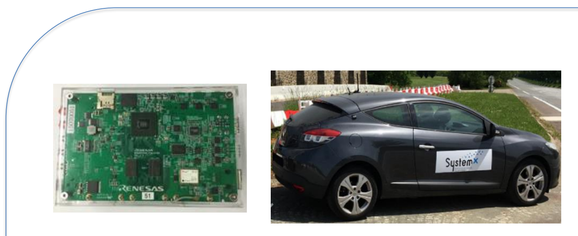
3. COMMUNICATION STACK AND PROFILES

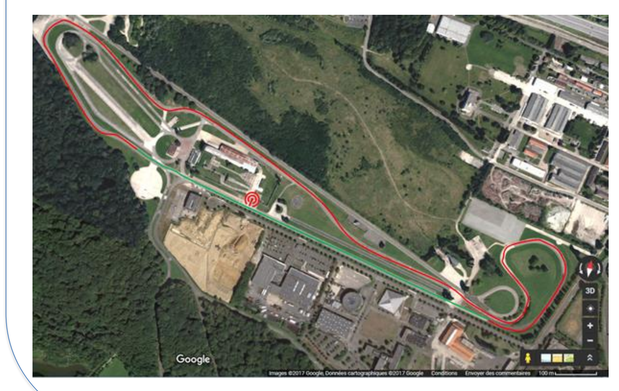
Profile TIG (unsecured):
TCP→IPv6→G5

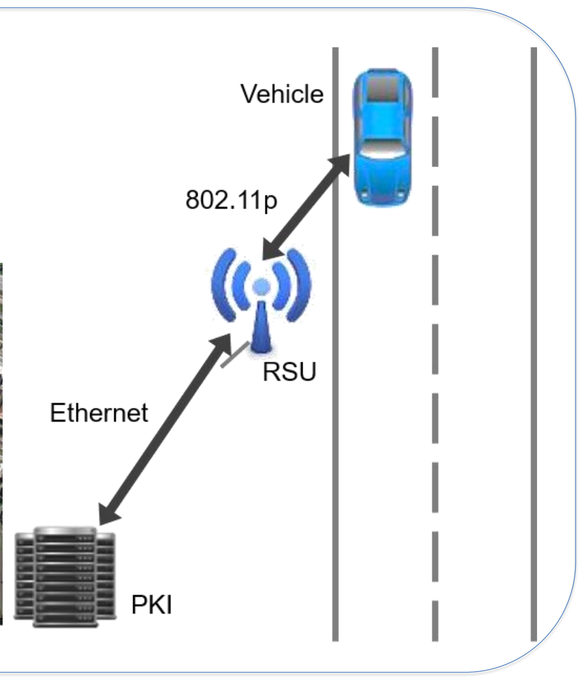
Profile TI3G (secured):
TCP→IPv6→ GN6ASL→GN→G5



4. USE CASE: AT RELOAD

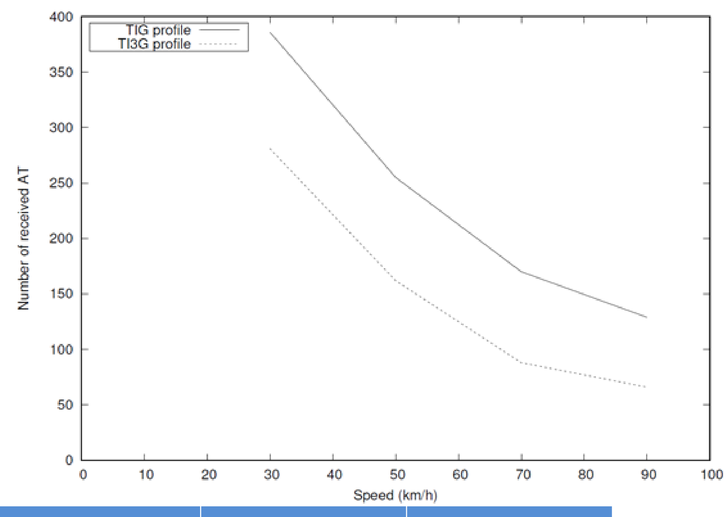






5. RESULTS

Number of AT reloaded **vs** speed



KPI		TIG	TI3G
Median AT request/response round-trip latency (ms)		440.051	728.657
Median packet size (Bytes)	Request	1073	1388
	Response	850	1166
Number of AT reloaded	30 (km/h)	390	260
	90 (km/h)	140	54

6. FUTURE WORK

Test the performance with an embedded Hardware Security Module (HSM) to improve latency of request creation and cryptographic operations.

REFERENCES

F. Haidar, A. Kaiser and B. Lonc, "On the Performance Evaluation of Vehicular PKI Protocol for V2X Communications Security," *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, Toronto, ON, 2017, pp. 1-5.

580 Sciences et Technologies de l'Information et de la Communication (STIC)
Telecom ParisTech
Farah HAIDAR- Farah.haidar@renault.com