STU FIIT
SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA
FACULTY OF INFORMATICS AND INFORMATION TECHNOLOGIES

Optimizing security of communication in the Internet of Things by OpenHip (E-HIP)

Master Thesis

Author: Peter Kaňuch
Supervisor: Dr. Dominik Macko

Computer Engineering
Internet Technologies
2018/2019

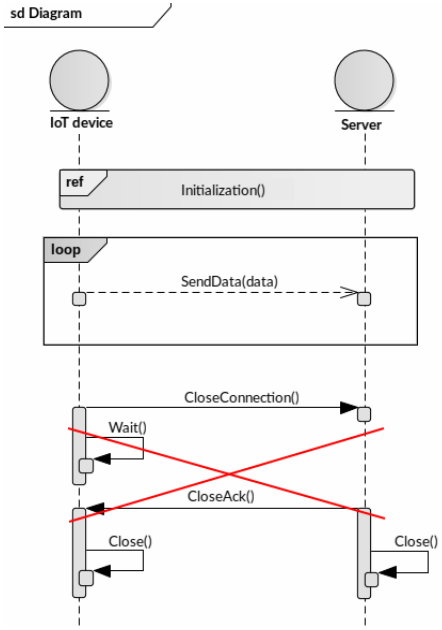
Presented at:
2019 42nd International Conference on Telecommunications and Signal Processing

Abstract

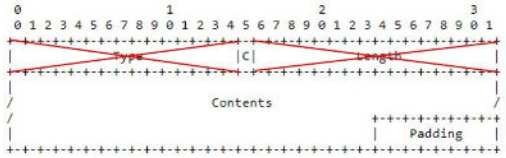
The research in the area of Internet-of-Things (IoT) security is still underway due to the growing IoT networks. The main goal of the existing works, optimizing security protocols, is to make them more efficient in order to reduce their energy requirements. The result is the extended lifetime of the device powered by a battery, while preserving all the security features of the protocol such as confidentiality, integrity, authenticity, etc. Based on the analysis, we have decided to focus on the protocol HIP (Host Identity Protocol), identified several optimization possibilities for efficient use in the IoT area, and proposed its modification. The resulting effect of the proposed optimization (E-HIP) has been evaluated experimentally, and it represents an increase in energy efficiency by about 20%.

The Proposed HIP Optimizations

Implemented proposal no. 1
- Removal of the CloseAck
- Removal of the Closing state



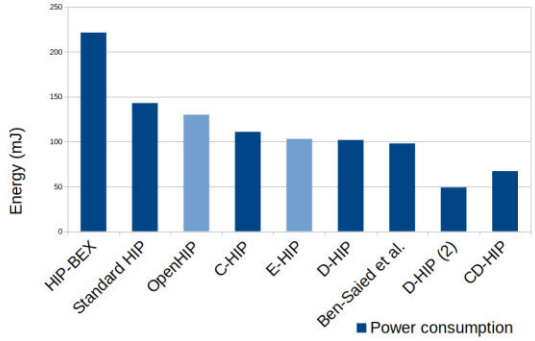
Implemented proposal no. 2
- Reduction of the parameter format (type, length)
- Reduction of the transmitted control messages



Implemented proposal no. 3
- Removal of the HI-R parameter (public key)
- Key in the device memory
- Reduction of the transmitted control message

Results

	RX bytes	TX bytes	Overall
OpenHip	1184	1048	2232
E-Hip	760	1032	1792
Optimization (%)	35,81	1,53	19,71



Conclusion

Te battery-powered device lifetime is still limited. This was the target of our work. The energy intensity of the proposed solution is comparable to other existing works. We can expect some contributions as reduction of network load, reduction of processor-time usage and reduction of energy required for communication. In our further work, we are going to test it in a real IoT network using a low-power communication technology for IoT/mMTC (e.g. Bluetooth Low Energy, NB-IoT, LTE CatM1, etc.). The future work can also bring some possibilities for improvement since there are still unimplemented parts of the proposed solution that could be incorporated or it can be combined with some existing optimizations (e.g. C-HIP, DHIP) and achieve even higher energy efficiency.

This research was partially funded by by the Slovak Research and Development Agency (APVV-15-0789), the Slovak Cultural and Educational Grant Agency (KEGA 011STU-4/2017), the project "University Science Park of STU Bratislava" (ITMS 26240220084), co-funded by the European Regional Development Fund, and the projects no. 2018/14427:1-26C0 and 002STU-2- 1/2018.