Power-Aware Security Protocols for the Internet of Things

Tiago Diogo

Instituto Superior Técnico, Avenida Rovisco Pais 1, Lisboa,
tiago.diogo@tecnico.ulisboa.pt

Abstract. The abstract should summarize the contents of the paper using at least 70 and at most 150 words.

Keywords:

1 Introduction

The Internet of Things (IoT) can be seen as web of interconnected devices that go from everyday wearable objects into fully deployed sensor networks. Despite the huge variety and characteristics of these devices, one thing that they all have in common in the constrained nature they're built uppon. In order to enable the massive deploy to be expected in the near future [1] IoT devices must be accessible and affordable, capable of operating under lossy wireless networks while being battery powered.

2 Main Goals

Given the constraints and limitations of IoT devices described in the previous chapter, the first objective of this work is to identify existing protocols at the OSI application layer that take into account those constrains and are design to allow communication between these devices without consuming an amount of resources that would be appropriate for standard devices but excessive for the IoT ones.

After the analysis of the existing solutions, a baseline of power consumption will be established. Then, the focus will move towards adding confidentiality to the transmitted information by securing the channel. Once both the application level protocols and proper security solutions are defined, experiments will be performed so that the added power consumption cost of adding the security layers can be measured, profiled and documented therefore enabling the finding of the best parameters for a desired level of security.

[1] http://www.gartner.com/newsroom/id/2636073

The work will then proceed towards finding effective counter-measures against a specific group of attacks that targets the IoT devices by intensifying the use of its resources therefore draining the available power and placing the node offline. The ultimate goal will is to propose an energy-efficient security mechanism that can resist these power-drain (a.k.a vampire) attacks.

3 Related Work

3.1 Protocol Analysis and Selection

3.1.1 Web Protocols

place here a study on web protocols, focus on http and show how it works and how spread it is. provide a study on resource consumption, laying the bed for the next section(iot protocols)

3.1.2 IoT Protocols

do a large analysis of mqtt, coap and 6lowpan protocols. provide tables with diferences between mqtt and coap from the study paper [1]

3.1.3 IoT Protocols Security and Improvements

related work regarding protocol improvements and security (citar aqui os papers fixes) coap security analysis (citar aqui que isto ainda não está a ir buscar sozinho e fazer à mão não pode ser)

3.2 Attack Analysis, Detection and Prevention

3.2.1 Internet Attacks

do some work identifying threats to the web in general

3.2.2 IoT Attacks

4 Proposed Solution

5 Work Evaluation

6 Work Planning

7 Conclusion

References

1. Ma, X., Valera, A., Tan, H.x., Tan, C.K.y.: Performance Evaluation of MQTT and CoAP via a Common Middleware. (April) (2014) 21–24