# 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://blogs.wsj.com/cio/2015/06/02/internet-of-things-market-to-reach-1-7-trillion-by-2020-idc/

*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 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

*pequeno texto inicial sobre este assunto, referir o paper que faz o survey sobre as soluções existentes de 2015 [1]*

***Hypertext Transfer Protocol (HTTP)***

*This is the resume about HTTP referir que é bom mas não está adaptado às necessidades dos aparelhos com poucos recursos*

***Constrained Application Protocol (CoAP)***

*This is the resume about CoAP referir o paper que mostra claramente que o coap consome menos recursos que o HTTP [2]*

***Message Queue Telemetry Transport (MQTT)***

*This is the resume about MQTT referir o paper que faz a comparação entre o mqtt e o coap mostrando que o coap é melhor (na maioria) [3] referir que foi desenvolvido o mqtt-sn [4] especifico para sensor networks*

*→ colocar aqui a tabela comparativa entre os 3 procotocolos ←*

*→ colocar aqui o desenho bonito das layers web vs layers IoT ←*

## 3.2 Security and Improvements

***Transport Layer Security (TLS)***

*This is the resume about TLS*

***Datagram Transport Layer Security (DTLS)***

*This is the resume about DTLS paper que diz mal do DTLS [5] e diz que outra solução é necessária*

## 3.3 Attack Analysis, Detection and Prevention

### 3.3.1 Internet Attacks

*do some work identifying threats to the web in general*

#### 3.3.2 IoT Attacks

*focus on the power-drain attacks alguns papers ainda não filtrados: [6, 7]*

## 4 Proposed Solution

## 5 Work Evaluation

## 6 Work Planning

## 7 Conclusion

## References


1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of Things: A Survey on Enabling Technologies, Protocols and Applications. IEEE Communications Surveys & Tutorials **PP**(99) (2015) 1–1
2. Savolainen, T., Javed, N., Silverajan, B.: Measuring Energy Consumption for RESTful Interactions in 3GPP IoT Nodes. (2014) 1–8
3. 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
4. Ibm: MQTT For Sensor Networks ( MQTT-SN ) Protocol Specification. (2013) 28
5. Alghamdi, T.a., Lasebae, A., Aiash, M.: Security analysis of the constrained application protocol in the Internet of Things. 2nd International Conference on Future Generation Communication Technologies, FGCT 2013 (2013) 163–168
6. Vasserman, E.Y., Hopper, N.: Vampire attacks: Draining life from wireless ad Hoc sensor networks. IEEE Transactions on Mobile Computing **12**(2) (2013) 318–332
7. Vanitha, K., Dhivya, V.: A Valuable Secure Protocol to Prevent Vampire Attacks In Wireless Ad Hoc Sensor Networks. **3**(3) (2014)