
# Internet of Things:

## Desafios de Segurança e Privacidade

# O que é a IoT?


A Internet of Things (IoT) é uma rede de dispositivos mecânicos e digitais que comunicam entre si trocando informação e dados úteis, sem que seja necessário intervenções humanas.

# Exemplos


- Uma pessoa estar numa determinada divisão da casa e a luz apagar-se quando a pessoa sai dela;
- Um frigorífico encomendar os alimentos que estão em falta;
- Um frigorífico sugerir o que podes cozinhar tendo em consideração os alimentos que nele existem;
- Receber uma notificação no telemóvel caso deixes a porta de casa aberta.

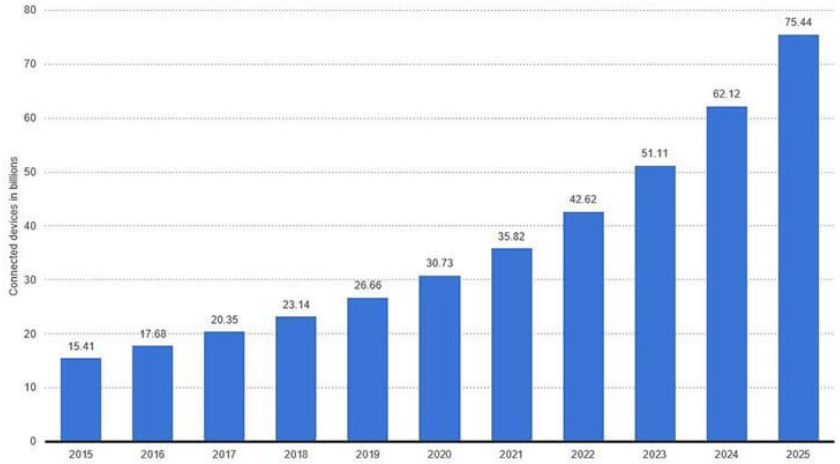
Universidade do Minho
Escola de Engenharia

O objetivo da IoT é automatizar e tornar a vida dos seres humanos mais confortável.

Universidade do Minho
Escola de Engenharia

Internet of Things - number of connected devices worldwide 2015-2025

## Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)




statista

# Principais tecnologias da IoT

Universidade do Minho
Escola de Engenharia

- *Electronic Product Code* (EPC);
- *Short-Range Wireless Technologies*:
  - *NFC*, *WiFI*, *Bluetooth*, *ZigBee*, *6LoWPAN* e *Ultra WideBand*;
- *Wireless Sensor Network*;
- *Cloud Computing*;
- *IPv6*;
- *Artificial Intelligence*.

# O que se pode esperar no futuro da IoT?

Universidade do Minho
Escola de Engenharia

- Mais sensores;
- Mais *Machine Learning*;
- Segurança reforçada;
- A privacidade dos dados se torne uma prioridade.

# Importância da Segurança e Privacidade


Áreas críticas onde a IoT é utilizada:

- Saúde;
- Localização;
- Sistemas Bancários;
- Infraestruturas (*e-health*, *e-banking system* e *smart buildings*).

Se os dados referentes a estas áreas forem de alguma forma comprometidos a privacidade do utilizador é afetada.

# Arquitetura da IoT


A IoT possui apenas de uma arquitetura genérica composta por 4 camadas:

- Camada de Percepção;
- Camada de Rede;
- Camada de Aplicação;
- Camada de *Middleware*.


Por não se tratar de uma arquitetura padronizada as diferentes camadas da IoT tornaram-se vulneráveis a diferentes tipos de ataques como por exemplo acessos não autorizados e vírus.

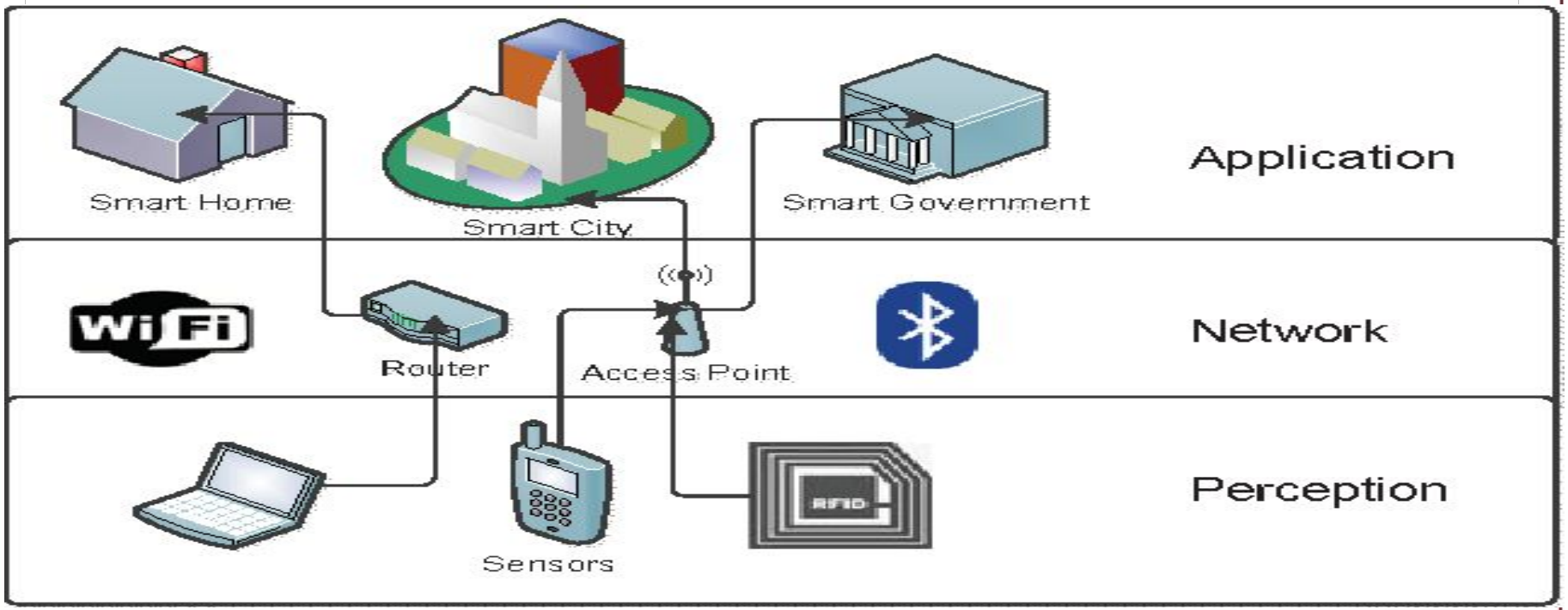
# Principais Desafios


**“Security by design is a mandatory prerequisite to securing the IoT macrocosm, the Dyn attack was just a practice run”**

— James Scott, Sr. Fellow, Institute for Critical Infrastructure Technology

# Camadas da IoT que podem ser afectadas

Universidade do Minho
Escola de Engenharia

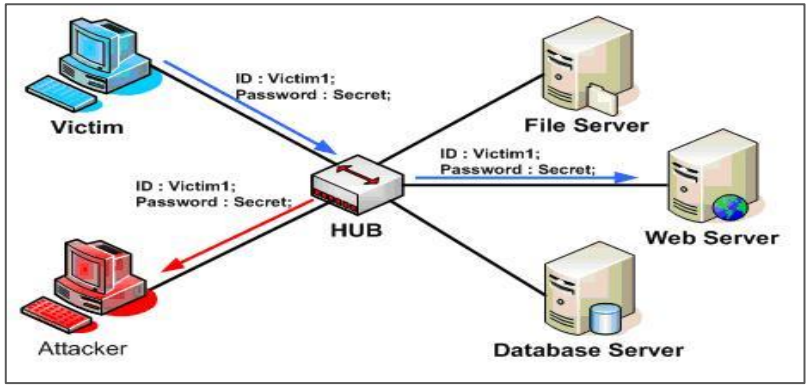


# Camada de Percepção

Universidade do Minho
Escola de Engenharia

- Dispositivos colocados em espaços públicos facilmente atacados fisicamente.

- Ataques de natureza invasiva podem pôr a nossa privacidade em causa (*eavesdropping attack*).

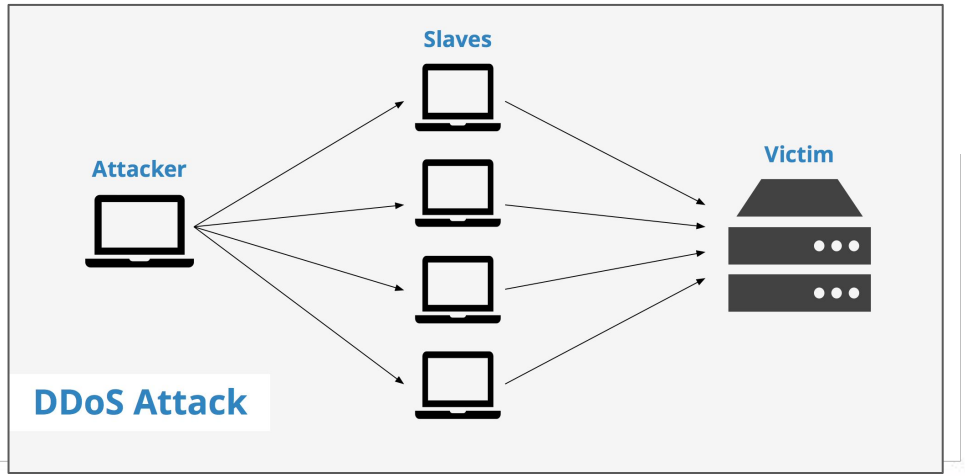


# Camada de Rede/*Middleware*

Universidade do Minho
Escola de Engenharia

- Ataques com objetivo de invalidar o sistema e destruir as comunicações entre dispositivos de receção e de envio.

- Exemplos destes ataques:
  DoS (*Denial of Service*).
  *Mirai Botnet*.



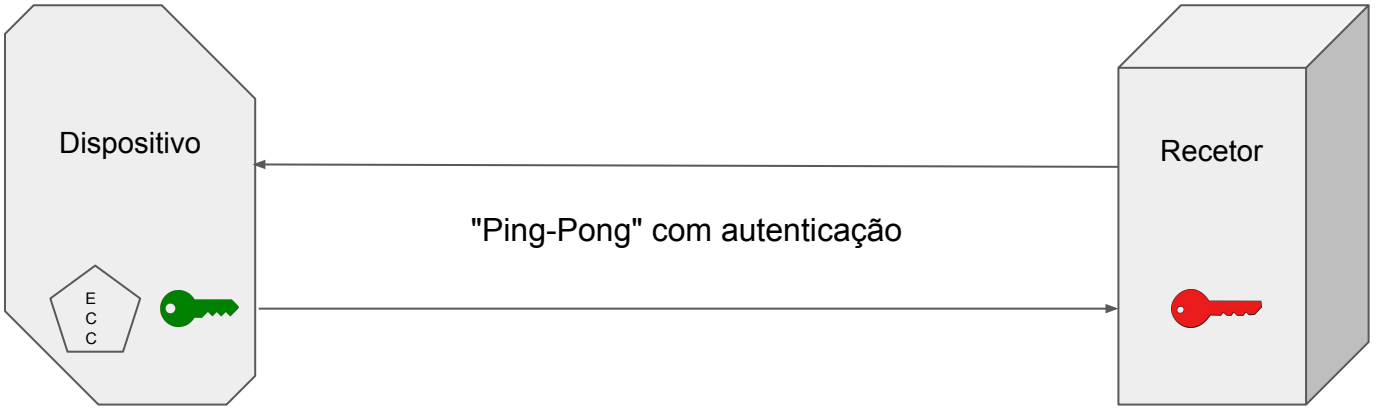
# Camada de Aplicação

Universidade do Minho
Escola de Engenharia

- Uso do protocolo CoAP (*Constrained Application Protocol*).
- Dependência da DTLS (*Data Transport Layer Security*) o que constitui um problema devido à sua falta de aperfeiçoamento.
- Perigo de fragmentação de mensagens e, consequentemente, perda de informação.

# Proposta

Universidade do Minho
Escola de Engenharia



# Encriptação

Universidade do Minho
Escola de Engenharia

# Elliptic Curve Cryptography

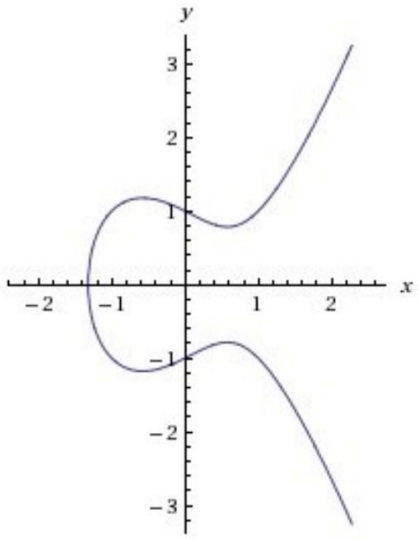

**Para a mesma força de segurança:**

**ECC vs RSA**

- 160-bits por chave vs 1024-bits por chave
- melhor performance
- menos complexidade computacional
- várias variantes

Standard equation for the elliptic curve:

$$E: y^2 = x^3 + ax + b$$



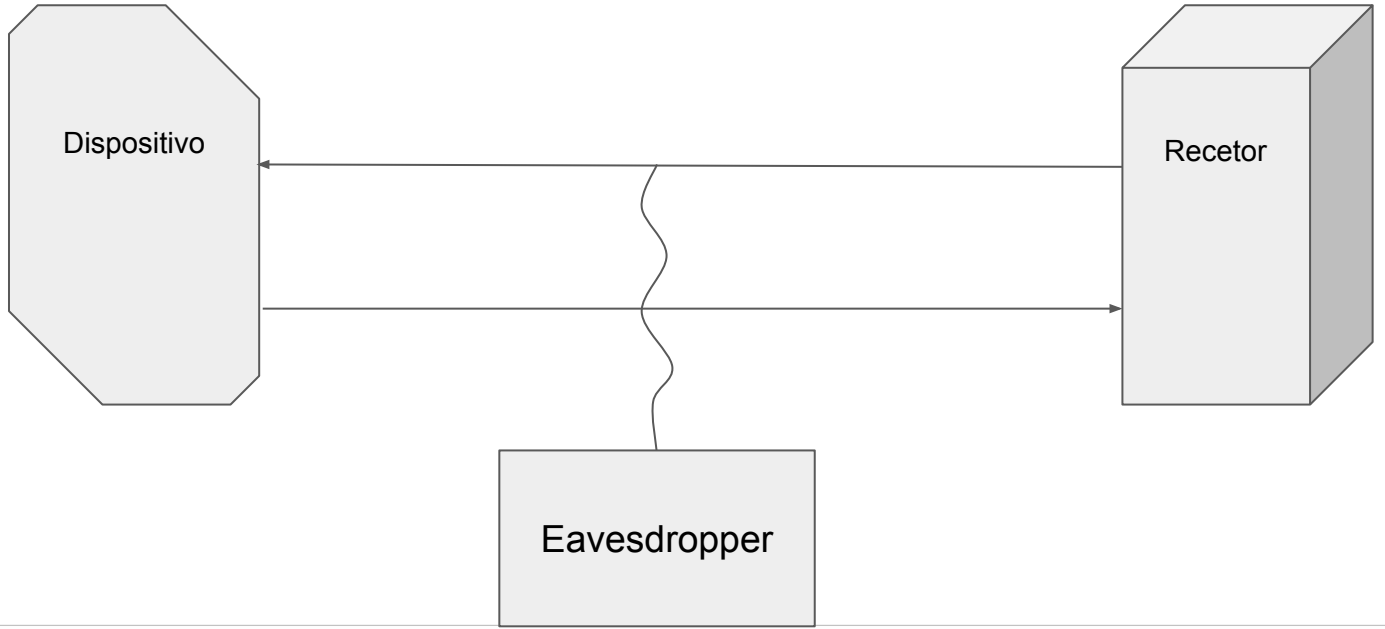

*E* where a = -1 e b = 1

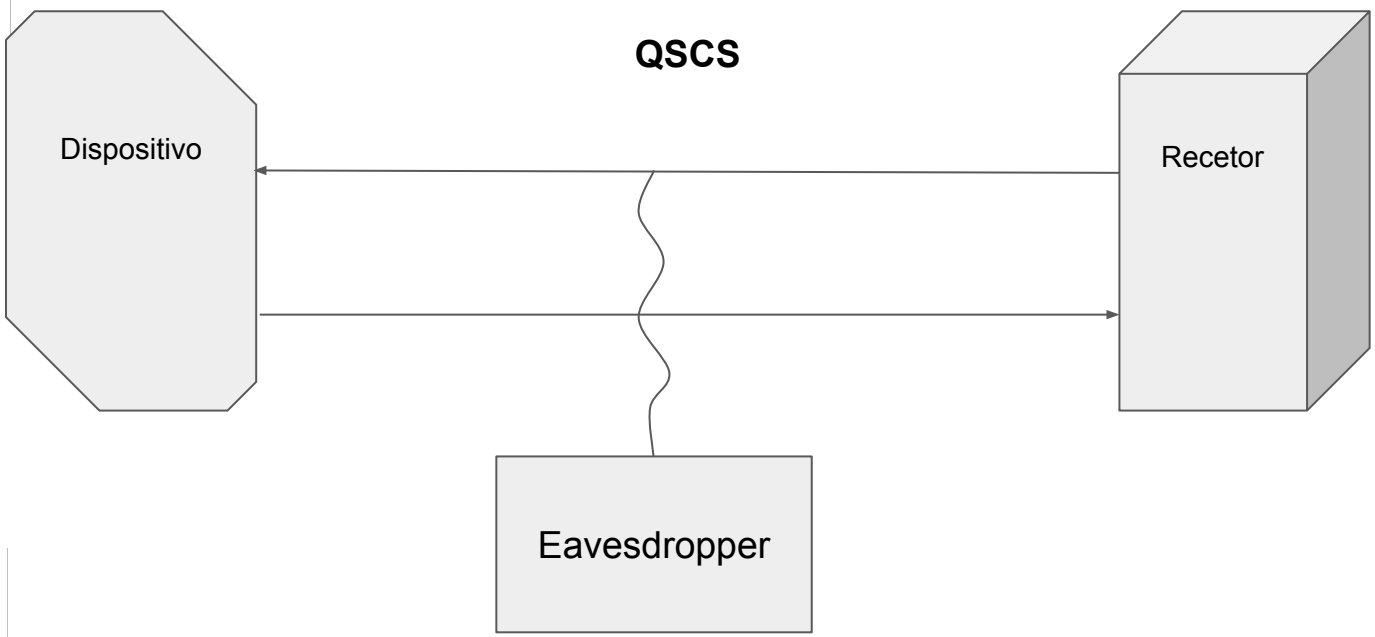

| Basic Operation | Average # of Cycles | Running Time |
|---|---|---|
| Addition | 957 | 0.422 µs |
| Shifting (2 * $k$) | 941 | 0.415 µs |
| Multiplication ($k$ * $k_2$) | 1,861 | 0.821 µs |
| Inversion | 15,300 | 6.750 µs |


# Algoritmo de Montgomery Ladder

# Quantum Secure Communication System

Universidade do Minho
Escola de Engenharia

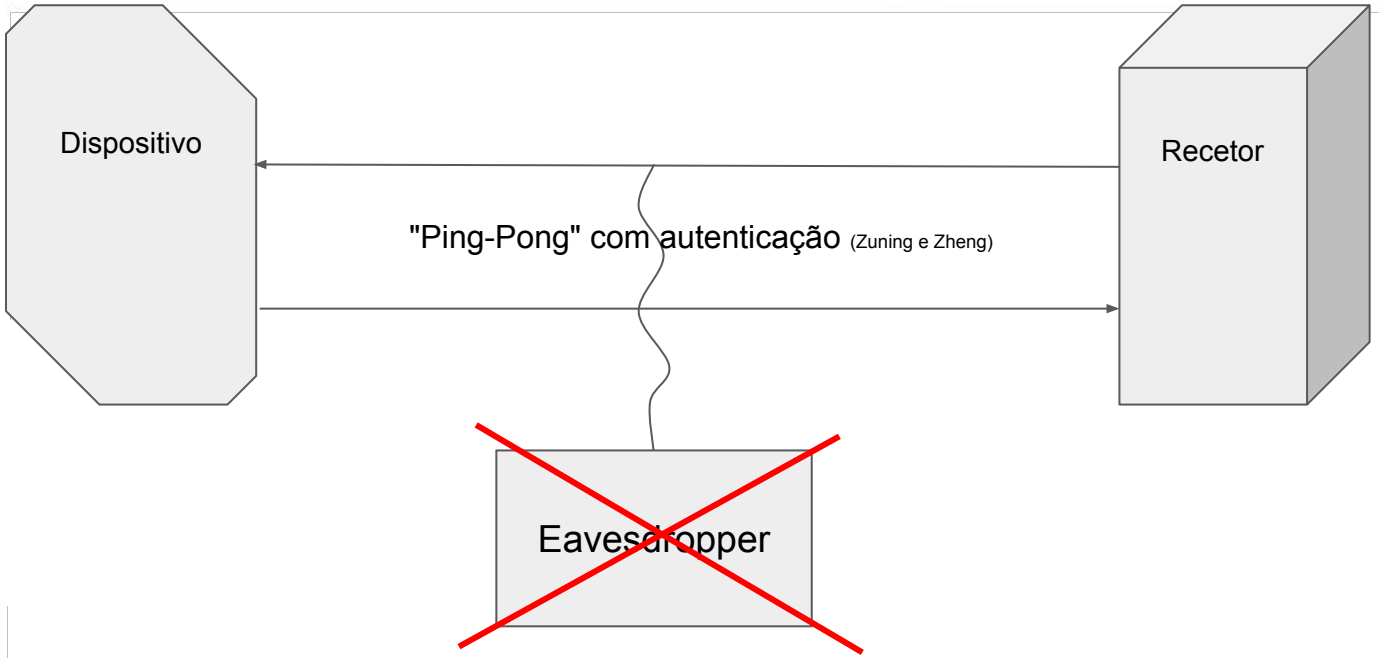





Universidade do Minho
Escola de Engenharia

Tempo máximo de deteção: 150μs (mínimo 20μs).

A um ritmo de transmissão de 10 Mbit/s, seria de 1500 bits de informação, o equivalente a 187.5 caracteres.




Universidade do Minho
Escola de Engenharia

Protocolo de aceitação de chaves braid-based

Controlo de medida do qubits

Envio assintótico de chaves e mensagens