Internet of Things: Desafios de Segurança e Privacidade

Catarina Machado, João Vilaça, and Ricardo Milhazes Veloso

Universidade do Minho, Departamento de Informática, 4710-057 Braga, Portugal
e-mail: {a81047, a82339, a81919}@alunos.uminho.pt

Resumo O presente ensaio escrito tem como objetivo introduzir o tema *Internet of Things* (IoT) e contextualiza-lo, apresentar e discutir os principais desafios associados ao mesmo tendo como foco o problema da segurança e da privacidade. Indicamos também alguns projetos atuais que têm a intenção de colmatar esse obstáculo através de técnicas eficientes que assegurem a privacidade e integridade tanto aos dispositivos IoT como aos utilizadores destes, que neste momento não é uma realidade. Daí as propostas de utilização de técnicas como *Elliptic Curve Cryptography* e *Quantum Secure Communication System*.
Existe uma necessidade clara de incutir segurança a estes dispositivos e por isso, também é necessário que as entidades que estão responsáveis pelo desenvolvimento da tecnologia da IoT tenham uma atenção reforçada a este tema.

1 Introdução

O atual ensaio escrito é sobre a *Internet of Things* (IoT), mais precisamente os desafios de segurança e privacidade nela inerentes. Deste modo, iremos esclarecer o conceito da IoT exemplificando-a com alguns exemplos aplicacionais e expondo também a sua crescente evolução (Secção 2.1). Apresentaremos os principais desafios da IoT salientando o problema da segurança e da privacidade, que é o principal objeto de estudo deste ensaio escrito (Secção 2.2). Em seguida, explicaremos quais são os problemas mais graves em termos de segurança e privacidade da IoT debruçando-nos sobre as principais camadas que a constituem e as principais ameaças a estas camadas (Secção 3). Por fim, terminamos com um conjunto de soluções que permitem, em paralelo, assegurar o eficaz e seguro funcionamento dos meios de comunicação entre os dispositivos de IoT e os recetores da informação, através de métodos criptográficos mais rápidos mas ainda assim seguros e novos protocolos de rede baseados em tecnologia quântica. A solução que propomos baseia-se na integração de várias soluções que em conjunto conseguem assegurar mais controlo numa área crítica da privacidade do indivíduo mantendo sempre em consideração o baixo poder computacional oferecido pelos dispositivos de IoT (Secção 4).

2 Contextualização

2.1 Geral

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[3]. O intuito da IoT é automatizar e tornar a vida dos seres humanos mais confortável. A grande vantagem é que pode ser usada nos mais diversos ramos do nosso dia a dia, e da nossa vida em geral, facilitando imenso a forma como a encaramos e como lidamos com as mais variadas adversidades e contratempos que eventualmente surgem.

Na prática, algumas aplicações da IoT podem ser, por exemplo, uma pessoa estar numa determinada divisão da casa e a luz apagar-se quando a pessoa sai da mesma, um frigorífico encomendar os alimentos que estão em falta ou 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, entre muitas outras. Torna-se assim notório que esta tecnologia está

a mudar o mundo, a forma como nós vivemos e pensamos, e a forma como as empresas se posicionam nos negócios[5]. Tal como se pode constatar no gráfico da Figura 1 esta tecnologia está a ser cada vez mais usada e a quantidade de dispositivos conectados está a aumentar substancialmente. Atualmente, temos cerca de 23 mil milhões de dispositivos conectados sendo que daqui a menos de 10 anos espera-se que este número triplique.

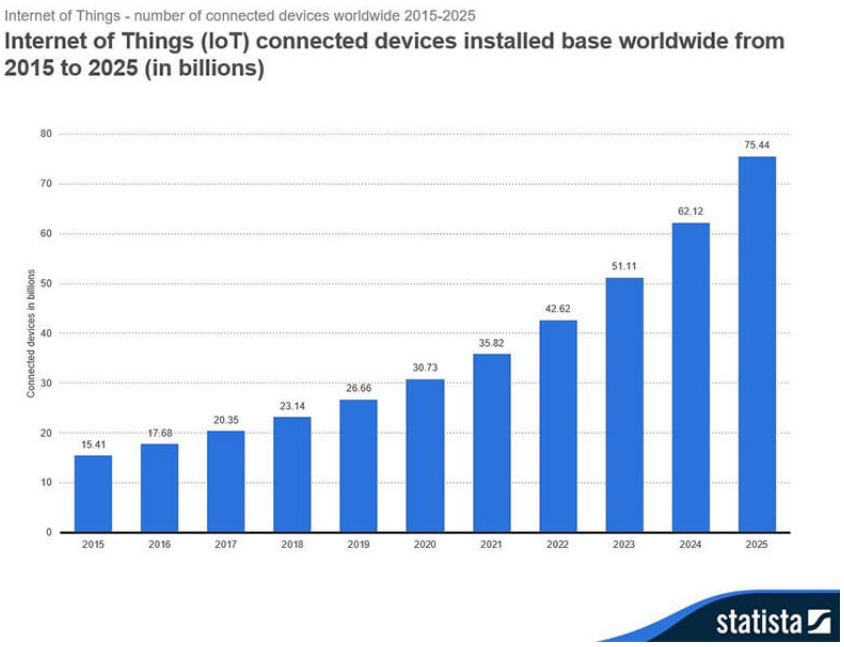

Figura 1. Número de dispositivos conectados na IoT.

As principais tecnologias da IoT são *Electronic Product Code (EPC)*, *Short-Range Wireless Technologies* (como por exemplo *NFC*, *WiFi*, *Bluetooth*, *ZigBee*, *6LoWPAN*, *Ultra WideBand*) e *Wireless Sensor Network*. Outras tecnologias de ponta usadas no desenvolvimento da IoT são *Cloud Computing*, *IPv6* e *Artificial Intelligence*[5]. Para o futuro, o que se pode esperar é que o número de sensores aumente, mais *Machine learning* nos dispositivos IoT, padrões físicos mais rígidos, segurança reforçada e que a privacidade dos dados se torne uma prioridade.

2.2 Específico

A quantidade de dados transferida entre dispositivos IoT e a sensibilidade da informação que estes dados contêm são dois aspetos importantes a serem considerados quando falamos sobre a segurança da IoT. Das imensas áreas da IoT existem várias que podem ser consideradas críticas tais como as relacionadas com passagem de informação relativa à saúde, à localização, sistemas bancários e infraestruturas (*e-health*, *e-banking system* e *smart buildings*). São consideradas críticas uma vez que se os dados referentes a estas áreas forem, de alguma forma, comprometidos será uma enorme falha de segurança relativamente à privacidade do utilizador[5].

A IoT não possui uma arquitetura uniforme e standard, dispondo apenas de uma arquitetura genérica composta por 4 camadas: a camada de percepção, a camada de rede, a

camada de aplicação e a camada de *middleware*[1]. Assim, 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. A IoT é tão simples de implementar que faz com que existam medidas habituais de segurança que não conseguem ser introduzidas[5].

3 Desafios de Segurança e Privacidade

Sendo a IoT uma extensão da Internet é fácil entender que os problemas de segurança e privacidade são um desafio enorme, isto porque a própria Internet não é segura o suficiente.

Ao mesmo tempo que se tentam resolver estes problemas existe uma necessidade quase inata de criar novas funcionalidades o que irá causar ainda mais problemas, por isso devíamos dar atenção e focarmo-nos nas fragilidades que existem na área da segurança. Infelizmente isto não é uma realidade pois as empresas, de forma a reduzir o custo, dão pouca importância a esta fase criando apenas soluções básicas e tradicionais (como firewall), o que não é o suficiente para proteger os dispositivos IoT. Para corrigir estas fragilidades temos primeiro que entender onde se encontram os problemas e os desafios associados à IoT.

3.1 Camada de Percepção

Os dispositivos IoT, como os sensores, encontram-se sempre no mesmo local. Exemplos destes são as smart TVs e as consolas que captam dados relativamente ao nosso quotidiano que podem ser partilhados ou visualizados.

Ataques Físicos Estes ataquem acontece mais ao nível do hardware dos dispositivos IoT. Sendo que bastantes destes dispositivos irão funcionar em zonas abertas, existe uma enorme suscetibilidade a ataques físicos[3].

Privacidade Existem imensos ataques diferentes, tal como o *eavesdropping attack* que é uma das principais ameaças à Camada de Percepção das IoT e à privacidade dos utilizadores destes dispositivos. Como a própria palavra indica, *eavesdropping* consiste em ter acesso ou "espiar"dados que estão a ser transmitidos entre os dispositivos de receção e de envio destes, portanto, se estes dados não forem devidamente protegidos através de mecanismos de criptografia o atacante pode entender, com facilidade, o conteúdo das mensagens[3][5].

3.2 Camada de Rede/*Middleware*

Os ataques a esta camada têm o objetivo de tornar o servidor que controla a passagem de dados entre a Camada de Percepção e a Camada de Aplicação não funcional, ou seja tornar os recursos do sistema indisponíveis para o utilizador. Ao contrário do *eavesdropping attack*, este ataque concentra-se mais em invalidar o sistema do que propriamente em invadi-lo. Exemplos deste tipo de ataques são os ataques DoS (*Denial of Service*) que podem utilizar técnicas para sobrecarregar o sistema ou então apenas obstruir a comunicação entre os dispositivos de receção e de envio[3].

É possível também fazer ataques do tipo DDoS (*Distributed Denial of Service*) que acabam por ser o mesmo que os DoS mas, como o próprio nome indica, são ataques coordenados. Estes ataques coordenados aproveitam-se de dispositivos frágeis (como são os

[1] Software que fornece serviços para aplicações de software além daqueles disponíveis pelo sistema operativo.

IoT) de forma a utilizá-los para atacar uma determinada vítima. Um exemplo muito conhecido destes ataques é o *Mirai Botnet* que utiliza bots (que já existem) para "recrutar"novos bots - dispositivos IoT - utlizando uma técnica simples de tentar cerca de 60 logins diferentes que, normalmente, são os logins de fabrico e que raramente são alterados por quem utiliza os dispositivos[7].

3.3 Camada de Aplicação

Nesta camada tem sido utilizada a CoAP (*Constrained Application Protocol*), que acaba por ser uma versão customizada e comprimida do conhecido protocolo HTTP. Na teoria, este protocolo será o futuro dos protocolos de aplicação; mas a sua utilização depende da DTLS (*Data Transport Layer Security*) e esta ainda tem falta de aperfeiçoamento. Um dos possíveis perigos associados a este protocolo é a fragmentação das mensagens e possível perda de informação[5].

4 Propostas

Com base nos problemas apresentados, sugerimos que a comunicação de dados dos dispositivos IoT use duas camadas adicionais de segurança de modo a impedir tanto o acesso aos dados comunicados através da rede como, em caso de falha deste primeiro, à sua leitura em texto claro. Neste modelo, o dispositivo IoT (a partir de agora mencionado como D1) está apenas ligado a um único recetor de informação (R1). O D1 teria um CPU dedicado unicamente para encriptar todos os dados que dele são enviados. Aquando do momento de configuração o utilizador terá de gerar chaves assimétricas, estilo RSA, e a chave pública ficará na posse do D1 e a privada na posse do R1, a única maneira de modificar o recetor da informação ou as chaves utilizadas terá de ser através de uma reinicialização de todas as configurações e dados do D1. Os algoritmos de encriptação de dados a comunicar serão adiante mencionados na subsecção 'Elliptic Curve Cryptography'. Em relação à transmissão de dados, propomos, com o principal objetivo de colmatar uma das maiores falhas de segurança relacionadas com IoT, o *eavesdropping attack*, um sistema de comunicação quântico[6], que deteta o ataque mas reforçado com a utilização de um protocolo "Ping-Pong"com autenticação[4] para comunicações multicanal que permite evitar o acesso de dispositivos não autorizados aos dados transmitidos autenticando mensagens.

4.1 Elliptic Curve Cryptography

Optar pela utilização deste tipo de método para além de possibilitar que os dados comunicados não fossem transmitidos em texto claro é possível aplica-los a um dispositivo IoT sem grandes custos adicionais. Tal como referido anteriormente, um pequeno CPU totalmente dedicado à criptografia de dados, como é feito, por exemplo, no caso do cartão de cidadão português, seria suficiente. Isto porque este recente método para cifra de dados assegura a mesma força de segurança que RSA com menos bits por chave (uma chave de 160-bit na ECC tem o mesmo nível de segurança que uma de 1024-bit na RSA[1]), ou seja, melhor *performance* e menos complexidade computacional[2], uma grande preocupação em IoT para reduzir tamanho e custos dos dispositivos.

Optando então por um algoritmo simples mas eficiente para implementar nos dispositivos de IoT sugerimos então um ECIES (*Elliptic Curve Integrated Encryption Scheme*) simplificado, que utiliza como argumentos do algoritmo a chave assimétrica pública do recetor e os dados a encriptar, devolvendo como resultado a mensagem cifrada e um ponto na curva elíptica. Para desencriptar a mensagem o algoritmo recebe como argumento o par retornado anteriormente e a chave privada do recetor e devolva os dados em texto claro[2]. A nível aritmético, relacionado com a escolha dos pontos da curva no processo de encriptação dos dados, a escolha tem de ser mais ponderada, temos sempre de optar por uma

solução robusta contra *side-channel attacks* mas que exiga pouca memória em termos computacionais. Assim a escolha que possa atender às duas necessidades seria o algoritmo de *Montgomery ladder*, que em cada iteração do seu ciclo interno calcula adições e dois *left shifts* (mas que, apesar de assegurar que não exista um *side-channel attack* resulta numa perda de performance de 30 a 40% [2]).

4.2 Quantum Secure Communication System

Apesar de ser ainda bastante recente e de se encontrar em fases iniciais de investigação esta tecnologia de comunicação poderá vir a revolucionar a forma como os dados são transmitidos na rede, com especial destaque para a segurança que desta tecnologia advém. Com a implementação de um protocolo "Ping-Pong"com autenticação e a consequente utilização de um canal quântico é possível reduzir logo à partida para o máximo de tempo de deteção de um *eavesdropping attack* de 150μs (máximo 150, mínimo 20), a um ritmo de transmissão de 10 Mbit/s, seria de 1500 bits de informação, o equivalente a 187.5 caracteres[6]. Este *leak* de informação deve-se ao cálculo de matrizes de 1500x1500 no algoritmo que demora algum tempo, em especial em hardware com pouca capacidade de processamento como é o caso dos dispositivos IoT. Mesmo assim, não sendo suficiente, a escolha de um protocolo mais complexo como o "Ping-Pong"com autenticação, não só em relação ao anterior mas também a outros meio de distribuição de dados através de canais quântico é fácil de justificar, tal como é defendido por Zuning e Zheng, porque neste modelo tanto a origem da informação como o recetor são capazes de detetar consultas à informação transmitida utilizando um protocolo de aceitação de chaves *braid-based*, com dois modos de operação em que é possível fazer um controlo de medida do qubits e autenticar as mensagens, assegurando o assintoticamente envio seguro de chaves e de mensagens entre os dois participantes[4].

5 Conclusão

Apesar da importância de manter os dispositivos IoT não só o mais baratos possíveis, como também mais rápidos, mais pequenos e com o menor consumo de energia possível, é essencial que não se descarte a segurança dos mesmos, nomeadamente dos dados que eles recolhem, de modo a garantir a privacidade dos seus utilizadores. Nesta ótica achamos que a solução que propomos é uma excelente conjugação destes vários fatores. As duas camadas de segurança apresentadas, *Elliptic Curve Cryptography*, para a cifra dos dados recolhidos pelo dispositivo IoT que apenas poderá ser descodificada pelo previamente configurado recetor da informação, e o *Quantum Secure Communication System*, através do Protocolo "Ping-Pong"com autenticação para proteger o envio de informação na rede principalmente contra *eavesdropping attack*, que apesar de conseguirem forte índices de segurança e capacidade de proteger a informação manteriam em termos aceitáveis as três maiores preocupações: custos, velocidade e consumo de energia.

Referências

1. G. V. S. Raju and Rehan Akbani: Elliptic curve cryptosystem and its applications (2003)
2. Iskandar Setiadi, Achmad Imam Kistijantoro, Atsuko Miyaji: Elliptic Curve Cryptography: Algorithms and Implementation Analysis over Coordinate Systems (2010)
3. Mohamed Abomhara, Geir M. Køien: Security and Privacy in the Internet of Things: Current Status and Open Issues (2014)
4. Chen Zuning, Qin Zheng: A “Ping-Pong” Protocol with Authentication (2015)
5. Zejun Ren, Xiangang Liu, Runguo Ye, Tao Zhang: Security and Privacy on Internet of Things (2017)
6. Stanislaw Rajba, Lukasz Wieclaw, Sergii Nikolaienko, Yevhen Vasiliu: Methods of Data Protection for Quantum Secure Communication System (2017)

7. Josh Fruhlinger : The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet (2018)