Smart Cities: Problemas de Segurança e Privacidade

Pimentel J., Gonçalves P., and Silva R.

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a80874,a82313,a81716}@alunos.uminho.pt

Abstract. Devido à evolução das tecnologias *IoT* e da constante preocupação com a eficiência nas sociedades atuais, tornou-se fundamental a utilização destas no melhoramento da eficiência do dia-a-dia de uma cidade, criando assim as chamadas *Smart Cities*. Graças à implementação destas tecnologias *IoT* no quotidiano das cidades, a privacidade e segurança dos seus habitantes tornou-se um problema, uma vez que existe uma grande fragilidade do conteúdo recolhido, podendo mesmo colocar em risco as vidas dos cidadãos, cujo quotidiano se pretendia melhorar. Existem, no entanto, tecnologias que podem vir a resolver estes aspetos mais precários, dentro dos quais se destacam o uso de *Blockchains* e *Machine Learning*. É, assim, expectável que, um dia, as vantagens superem os riscos associados a estas cidades.

1 Introdução

A "*Internet* das coisas" (*IoT*) tem vindo a ser um paradigma revolucionário da comunicação que tenciona gerar uma imensa "grelha" de conexão de dispositivos digitais com a *Internet*, fazendo desta algo mais imersivo e universal [1]. Desta forma, com o tremendo crescimento do paradigma em questão, seria de esperar que diversos fatores do dia-a-dia fossem incorporados no mesmo, daí o aparecimento de *Smart Cities* (*SC*).

Sendo assim, uma *Smart City* refere-se a um ecossistema caracterizado pelo intenso uso de tecnologias de comunicação e informação (*Internet* das coisas), de gestão urbana e ação social dirigidas por dados (*Data Driven Urbanism*), de modo a fazer das cidades espaços mais atrativos, sustentáveis e locais únicos para inovação e desenvolvimento empresarial [2].

Como mencionado anteriormente, uma estrutura unificada para gestão de dados é fundamental para uma *SC* e todas as suas aplicações. Deste modo, um requerimento essencial para um bom funcionamento e eficiência de uma cidade destas passa pela manutenção e entrega de produtos de alta qualidade, como comida, água e energia. Seja o exemplo de uma integração inteligente da gestão e produção de alimentos com monitorização contínua da qualidade dos mesmos. Esta situação pode limitar e/ou detetar significativamente a propagação de doenças mortais e bactérias [3].

De igual modo, a manutenção inteligente da água da cidade pode detetar microrganismos e poluentes nocivos, alertando as autoridades municipais antes da disseminação de doenças. Outro exemplo benéfico passaria por recorrer a uma produção energética inteligente, podendo gerir a produção de energia com base nas necessidades variáveis na cidade.

No entanto, há obstáculos tremendos relacionados com as *Smart cities* [4], especialmente no que toca à privacidade e proteção de dados dos cidadãos, como será retratado ao longo deste artigo.

2 Privacidade e Segurança de Dados

Milhões de dispositivos recolhem, guardam e processam constantemente informação, com a ajuda de sensores espalhados pelos mais diversos equipamentos (Fig. 1). Devido à variedade de dispositivos e, consequentemente, sensores, a manutenção da segurança de dados e dos utilizadores torna-se um problema grave [3]. Em consequência destas fragilidades dos componentes presentes nas *SC*, estas tornam-se um alvo fácil de ataque.

Um dos principais fatores que originam este tipo de vulnerabilidades é utilização de equipamentos com baixo poder computacional e criptográfico, tipicamente presente em dispositivos de *IoT*, dando origem a pontos de entrada para malfeitores tomarem partido da informação presente nos instrumentos que fazem parte da *SC* [5].

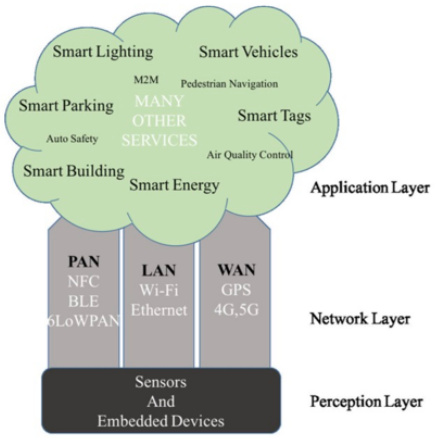

Fig. 1. *Layers* de uma *Smart City*.

2.1 *Smart Grids*

Numa época em que o aumento da eficiência na produção e utilização de recursos é uma necessidade para a sociedade, a implementação de um sistema que controle, de forma eficiente, estes recursos é algo crucial.

Um exemplo onde estes sistemas são aplicados é no fornecimento de eletricidade para os consumidores, levando à criação de *Smart Grids* (*SG*) [6]. Nestas existem canais de comunicação entre o consumidor e o distribuidor, que suportam *Advanced Metering Infrastucture, Demand Response, Distribution Grid Management* e *Wide Area Situation Awareness* [7].

Apesar do aumento da eficácia, tanto ao nível de produção, como de distribuição, estas *SG* são mais suscetíveis a ataques comparativamente a *grids* eléctricas tradicionais, em virtude do uso de *software SCADA* (Sistemas de Supervisão e Aquisição de Dados) para a monotorização do sistema. Independentemente de fornecer uma boa *performance*, estes *softwares* não foram construídos com o intuito de serem seguros [8]. Foram encontrados mais de 60.000 sistemas *SCADA* vulneráveis na *Internet*, o que demonstra a insegurança presente nas *SG* [9].

Como estas *grids* se estendem por vários de quilómetros, com várias subestações de controlo, as últimas tornam-se pontos de entrada no sistema, podendo provocar graves falhas no fornecimento de eletricidade às cidades ligadas na *grid*, afetando os seus habitantes diretamente.

2.2 *Smart Mobility*

Smart Mobility (*SM*) é a aplicação de tecnologias *ICT* (Tecnologias de Comunicação e Informação) na resolução dos problemas relacionados com os transportes (ex: poluição, acidentes, trânsito), tendo como objetivo principal o aumento da segurança nas estradas [3].

Apesar de todos os benefícios que a *SM* traz, esta produz bastantes desafios ao nível de segurança, que podem ter impacto direto na vida das pessoas. Basta que um invasor aceda aos sistemas que gerem semáforos, ou que controlem veículos, afetando os seus sistemas de *cruise control* adaptativos, de forma a causar o caos nas estradas, entre outras situações possíveis.

Estes problemas são originados, essencialmente, pela necessidade de colaboração entre várias tecnologias bastante distintas entre si [10].

2.3 *Smart Homes*

A evolução dos equipamentos de *IoT* levou a que fossem regularmente utilizados para controlar habitações e aspetos relativos às mesmas. Especula-se que dentro de poucos anos será possível controlar todos os aspetos de uma casa através da *Internet*, o que levanta grandes preocupações ao nível da segurança e privacidade dos seus habitantes.

Num estudo realizado em 2016, levado a cabo por investigadores da Universidade do Michigan [11], relativamente a aplicações sobre *Smart Things* da *Samsung*, foi demonstrado que cerca de 55% dessas possuem permissão sobre requisitos não necessários ao seu funcionamento. Estas podem, depois, ser exploradas por *malware*, pondo em risco a segurança e privacidade dos utilizadores.

Em 2017, a *WikiLeaks* revelou documentos comprovativos de que a *CIA* possui, neste momento, a capacidade de piratear qualquer dispositivo ligado à *Internet* numa habitação. Isto demonstra o quão desprotegida está a privacidade dos utilizadores, numa época onde estas casas são cada vez mais populares.

Apesar da comodidade que as *Smart Homes* proporcionam, estas trazem grandes problemas a nível de privacidade num local onde esta deveria ser dada como certa. Sendo assim, a sua implementação traz um risco elevado em termos de segurança, caso a privacidade dos utentes não seja posta em primeiro lugar.

3 Possíveis soluções

Existem algumas tecnologias e métodos que podem resolver alguns dos principais problemas associados a este novo conceito, como os mencionados acima, relativos a segurança e privacidade dos usuários.

Sabendo que os sistemas de *IoT* consistem em sensores e dispositivos com poder computacional limitado, baseados em algoritmos criptográficos fracos e embutidos em ambientes que comunicam através de tecnologias *wireless*, estes possuem numerosos problemas de segurança que necessitam de ser resolvidos [3]. Além disso, a existência destes sensores limita a quantidade de chaves criptográficas, pondo em causa a confidencialidade e integridade dos dados [5].

Uma ferramenta poderosa para contrariar os desafios mencionados é o standard *Trusted Platform Module* (*TPM*) [12], um módulo de *hardware* dedicado para operações de processamento criptográfico [3]. É usualmente utilizada como co-processador, tendo como objetivos a geração de números aleatórios para propósitos de encriptação, inicialização segura e selagem de dados. A *TPM* salva uma *hash* com o estado desejado da plataforma numa área segura e, sempre que o sistema é inicializado, verifica o estado atual comparativamente ao desejável. Caso sejam detetadas alterações, a inicialização do sistema é interrompida, sendo que, juntamente com a *BIOS*, é criada uma *root-of-trust* [3] (conjunto de funções no módulo computacional que é sempre confiável pelo sistema operativo). O uso de *TPM*

pode aumentar, exponencialmente, a integridade e confidencialidade do sistema, sendo uma solução viável para dispositivos que suportem tal hardware [3].

Já *Network Overlays* (Fig. 2) são uma boa solução para proteger a segurança e a privacidade nas redes com sensores e dispositivos que têm capacidades criptográficas limitadas, ou até inexistentes, isolando a rede em questão de possíveis atacantes [3].

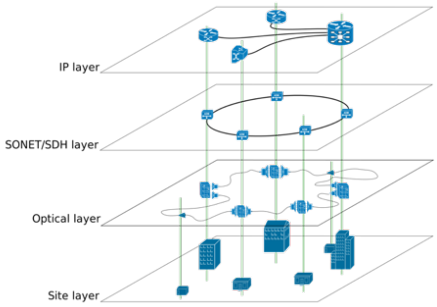

Fig. 2. Exemplo de um overlay de rede.

De igual modo, manter a privacidade do utilizador num ambiente de *SC* é muito mais complexo comparativamente a sistemas tradicionais, graças à existência de sensores de coleta de dados omnipresentes. Devido a isto, a acumulação de dados pessoais, indefinidamente retidos pelos servidores, pode pôr em causa a privacidade dos utilizadores.

Outro método passa pelo uso de *Blockchains* [13], sendo que estas podem resolver os problemas de pirataria até agora mencionados, tendo, ainda, potencial para erradicar todas as ameaças relativas à falta de privacidade nas cidades [3].

Inicialmente, ficaram famosas por serem a forma de acompanhar e transacionar a famosa criptomoeda, *Bitcoin* [14]. Além disso, sabendo que a sua *database* distribuída pode ser utilizada para registar qualquer tipo de transação segura e anónima, o seu maior benefício é a sua natureza *unhackable*. De modo a comprometer o sistema, é necessário piratear 51% dos nodos da rede, algo essencialmente impraticável [3].

Sendo assim, as *Blockchains* podem ser utilizadas, neste contexto, para estabelecer relações entre prestadores de serviços e utilizadores, usando contratos inteligentes, sem qualquer envolvimento de terceiros e renegociações. Por exemplo, um prestador de serviços pode fornecer bens aos utentes e observar a localização dos mesmos com auxílio de uma *Blockchain*. As pessoas podem, automaticamente, pagar aos credores, através do uso de uma *Blockchain* associada às suas contas bancárias, de forma segura. Um contrato inteligente deste teor traria transações consideravelmente mais rápidas, e, ainda, manteria a privacidade assegurada [3].

Outro problema em estudo nas *SC* são as vulnerabilidades de *Machine Learning* em ambientes hostis. Isto afeta *Intrusion Detection Systems* (*IDSs*), já que a sua tecnologia se baseia extensivamente em sistemas de *Machine Learning* para manter as redes seguras contra ataques complexos. De modo a melhorar a performance dos *IDSs*, os seus algoritmos são treinados em *datasets* chamados *adversarial samples*, ou seja, padrões e comportamentos de atacantes já conhecidos [3].

Tenha-se, a título de exemplo, a marcação de *emails* como *spam*. Esta marcação é feita através da procura de palavras-chave, contidas no correio de *spam* anteriormente recebido [3]. Com a maturação dos algoritmos de *Machine Learning*, os ataques também se tornam mais sofisticados, de modo a quebrar as barreiras erguidas, sem serem detetados. Os atacantes sabem que os algoritmos requerem treino, então realizam ataques direcionados ao envenenamento dos dados de treino, tornando os algoritmos inúteis [3].

Como é de notar, as soluções atuais não eliminam, completamente, todas as vulnerabilidades, sendo necessária mais pesquisa, de modo a serem encontrados métodos mais viáveis e sólidos.

4 Conclusão

Sabendo que o principal objetivo de uma cidade é melhorar a qualidade de vida dos seus habitantes, reduzir os custos de vida e gerar um ambiente sustentável, também o de uma *SC* o é. De modo a conseguir alcançar estes objetivos, é necessário superar alguns problemas de segurança que podem pôr em causa os direitos básicos dos cidadãos.

Apesar disto, ainda existem demasiadas fraquezas que podem ser facilmente exploradas por atacantes, numa tentativa de roubo e/ou deturpação de dados pessoais, adulteração de sistemas secundários regulados pelo sistema principal, entre outras situações.

Em suma, os benefícios deste novo tipo de cidades irão superar, em grande quantidade, os seus riscos, assim que os direitos dos seus usuários sejam completamente protegidos. Isto leva a que seja necessário um debate constante sobre as implicações da possível falta de segurança em comparação com as melhorias no quotidiano das pessoas.

References

1. A. Zanella et al., "Internet of Things for Smart Cities," IEEE Internet of Things J., vol. 1, no. 1, 2014, pp. 22–32.
2. J. Gubbi et al., "Internet of Things (IoT): A Vision, Architec- tural Elements, and Future Directions," Future Generation Computer Systems, vol. 29, no. 7, 2013, pp. 1645–60.
3. Smart Cities: A Survey on Data Management, Security and Enabling Technologies, Ammar Gharaibeh, Member, IEEE, Mohammad A. Salahuddin, Member, IEEE, Sayed J. Hussini, Student Member, IEEE, Abdallah Khreishah, Member, IEEE, Issa Khalil, Member, IEEE, Mohsen Guizani, Fellow, IEEE, and Ala Al-Fuqaha, Senior Member, IEEE
4. E. M. Biggs, E. Bruce, B. Boruff, J. M. Duncan, J. Horsley, N. Pauli, K. McNeill, A. Neef, F. Van Ogtrop, J. Curnow et al., "Sustainable development and the water–energy–food nexus: A perspective on livelihoods," Environmental Science & Policy, vol. 54, pp. 389–397, 2015.
5. L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.
6. NIST, "Framework and Roadmap for Smart Grid Interoperabil- ity Standards," Smart Grid and Cyber-Physical Systems Pro- gram Office and Energy and Environment Division, Engineering Laboratory, National Institute of Technology, U.S. Dept. of Commerce, Tech. Rep., 2014
7. N. Saputro, K. Akkaya, and S. Uludag, "A survey of routing protocols for smart grid communications," Computer Networks, vol. 56, no. 11, pp. 2741–2771, 2012.
8. V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," Computers & Security, vol. 25, no. 7, pp. 498 – 506, 2006.
9. A. Mirian, Z. Ma, D. Adrian, M. Tischer, T. Chuenchujit, T. Yardley, R. Berthier, J. Mason, Z. Durumeric, J. A. Hal- derman et al., "An internet-wide view of ics devices," in 14th IEEE Privacy, Security, and Trust Conference (PST16), 2016.
10. F. Kargl, "Vehicular communications and VANETs," in Talks 23rd Chaos Communication Congress, 2006, E. B. Hamida, H. Noura, and W. Znaidi, "Security of coop- erative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures," Electronics, vol. 4, no. 3, pp. 380–423, 2015.
11. E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in 2016 IEEE Symposium on Security and Privacy (SP), 2016, pp. 636–654.
12. T. Morris, Trusted Platform Module. Boston, MA: Springer US, 2011, pp. 1332–1335. [Online]. Available: http://dx.doi.org/10.1007/978-1-4419-5906-5 796
13. M. Swan, Blockchain: Blueprint for a new economy."O'Reilly Media, Inc.", 2015.
14. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.