REDES SEM FIO E COMUNICAÇÃO MÓVEL

Eduardo Scheffer Saraiva

SAGAH
SOLUÇÕES EDUCACIONAIS INTEGRADAS

Fundamentos da tecnologia sem fio

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Identificar as principais vantagens das redes sem fio.
- Descrever aspectos relacionados à segurança das redes sem fio.
- Reconhecer as principais ferramentas e *gadgets* para redes sem fio.

Introdução

As redes de comunicação sem fio vêm revolucionando a maneira como geramos, administramos e transmitimos dados. Esses sistemas apresentam grande abrangência, desde redes de comunicação industrial até aplicações domésticas, que já adotam redes sem fio para a comunicação de dados. Muito disso se deve ao baixo custo das redes sem fio em relação às redes cabeadas, que exigem dos usuários a reforma ou confecção de estruturas físicas, que aumentam o valor agregado da instalação.

Entretanto, com o aumento do número de redes sem fio e o avanço das tecnologias de comunicação, muito tem sido discutido em relação à segurança dessas redes. Essa preocupação cresce ainda mais com a popularização da tecnologia da internet das coisas (IoT, Internet of Things), que possibilita que objetos possam se comunicar e ser controlados por outros objetos sem a intervenção humana direta. Assim, surge no mercado um crescimento das buscas por profissionais capacitados e com conhecimentos tanto de segurança quanto de estruturação da rede sem fio.

Neste capítulo, você vai estudar os fundamentos das redes sem fio. Você vai ver quais são os aspectos positivos e negativos dessas redes e conhecer seus principais dispositivos e ferramentas. Também vai ver os aspectos e discussões a respeito da segurança nesse tipo de sistema.

1 Redes sem fio

As redes sem fio são uma realidade presente em nosso dia a dia, mas também em nosso futuro. Essas redes fornecem diversas vantagens em relação às redes convencionais (cabeadas), como mobilidade dos usuários da rede, rápida instalação, flexibilidade de redes e menor custo agregado, uma vez que não estão limitadas pelo cabeamento. Com todas essas importantes características, as redes sem fio revolucionaram a maneira como nós nos comunicamos, e o desenvolvimento de novas tecnologias no setor promete facilitar ainda mais nossas vidas.

Para entendermos melhor o funcionamento dessas redes, podemos dividir a estrutura da rede em diferentes elementos, de modo a compreender o papel de cada elemento no conjunto. Acompanhe (KUROSE; ROSS; ZUCCHI, 2007):

- **Hospedeiro sem fio:** dispositivo que executa as aplicações dos usuários da rede. Os hospedeiros sem fio normalmente aparecem como *notebooks*, *smartphones* ou computadores de mesa.
- **Estação base:** é responsável pela transmissão e receptação dos dados dos hospedeiros da rede sem fio à qual pertence e funciona como um canal de comunicação entre o hospedeiro e a rede maior que o hospedeiro deseja comunicar. Normalmente, a estação base coordenada a comunicação de diversos dispositivos simultaneamente. Exemplos de estação base são as torres celulares e os pontos de acesso em LANs (*local area network*).
- **Enlace sem fio:** hospedeiros podem se conectar à estação base por meio de enlaces de comunicação sem fio. Esses enlaces são normalmente utilizados para conectar a rede sem fio a uma rede de maior porte. Além disso, eles podem ser utilizados dentro de uma rede para conectar diferentes dispositivos, como roteadores, comutadores e demais equipamentos de rede.
- **Infraestrutura de rede:** rede maior com a qual a rede sem fio se comunica.

Além dos elementos presentes nas redes sem fio, é importante conhecermos os diferentes tipos de comunicação existentes, que você pode observar no Quadro 1. Cada tipo de comunicação apresenta suas peculiaridades, que deverão estar de acordo com a aplicação ideal para o cliente.

Quadro 1. Tipos de comunicação sem fio

Tipo de comunicação	Descrição
Rádio	Primeiro tipo de comunicação sem fio, utiliza ondas de rádio, que partem de uma torre de transmissão para antenas receptoras sintonizadas na mesma frequência.
Comunicação telefônica	Um dos maiores exemplos de comunicação sem fio na atualidade, este sistema utiliza ondas de rádio de modo a estabelecer a comunicação entre as torres de transmissão e o aparelho telefônico.
Infravermelho	Este sistema de curto alcance transmite a informação de um dispositivo transmissor para um dispositivo receptor por meio de radiação infravermelha.
Bluetooth	Esta tecnologia de comunicação permite que diferentes dispositivos sem fio transmitam dados entre si.
Comunicação via satélite	Amplamente abrangente, esta tecnologia permite que usuários separados por grandes distâncias possam estabelecer uma comunicação.
Wi-Fi	Comunicação de grande popularidade, utiliza um roteador para administrar a comunicação entre diferentes dispositivos e a rede cabeada.

Outro aspecto importante das redes sem fio é quanto a sua estrutura, que pode ser dividida em estrutura de rede *ad hoc* e rede infraestruturada (KUROSE; ROSS; ZUCCHI, 2007). A **estrutura de rede *ad hoc*** é constituída pela comunicação por dispositivos próximos, utilizando meios de comunicação de baixo alcance, como infravermelho e *Bluetooth*. A estrutura *ad hoc* pode ser observada na Figura 1.

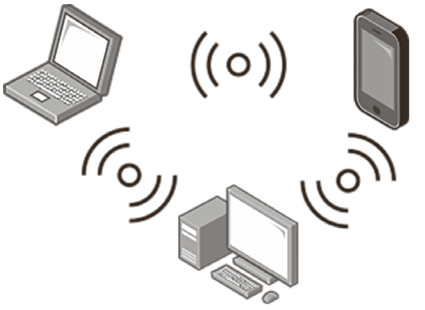

Figura 1. Estrutura de rede *ad hoc*.
Fonte: Adaptada de Pasqualini e Marcondes (2012).

Já para a **rede infraestruturada** é necessário um equipamento capaz de gerenciar e conectar a rede sem fio à rede maior, como a internet. Este tipo de estrutura permite a criptografia das informações, além de poder autenticar os diferentes usuários e dispositivos que desejam se comunicar com a rede (PASQUALINI; MARCONDES, 2012). Acompanhe a estrutura infraestruturada na Figura 2.

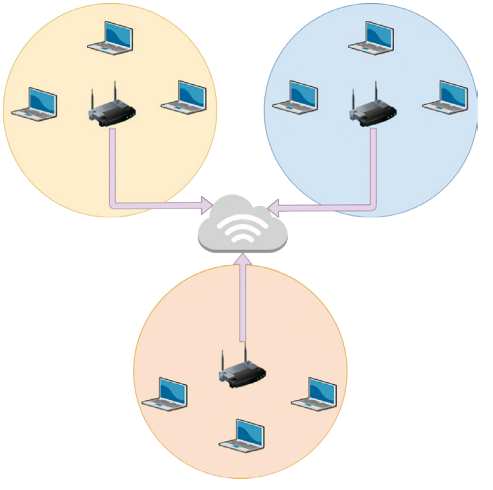

Figura 2. Rede infraestruturada.
Fonte: Adaptada de Kurose, Ross e Zucchi (2007).

Uma vez que entendemos os meios de comunicação possíveis para as redes sem fios, os elementos que as compõem e os tipos de estrutura de rede usualmente adotadas podemos estabelecer um comparativo entre as redes sem fio e as redes cabeadas, de modo a justificar a adoção desse tipo de tecnologia. O Quadro 2, a seguir, apresenta as vantagens e desvantagens da rede sem fio quando comparada com a rede cabeada.

Quadro 2. Vantagens e desvantagens das redes sem fio em relação às redes cabeadas

Vantagens	Desvantagens
Manutenção e instalação de baixo custo	Comunicação suscetível a interferências que fogem do controle do administrador da rede
Facilidade de acesso, necessitando apenas da existência de sinal	Facilidade de acesso também para pessoas desautorizadas, o que pode colocar em risco a integridade das informações
Mobilidade do usuário	Instalação da infraestrutura de redes maiores pode ser complexa
Atende mais usuários sem necessitar de mais equipamentos	Velocidade e alcance da transmissão normalmente menores do que em redes cabeadas

Nesta seção, você estudou os tipos de comunicação sem fio e as vantagens das redes sem fio em relação às redes cabeadas. Além disto, pode ter ideia dos elementos que compõem uma rede sem fio e dos tipos de estrutura.

2 Segurança e privacidade

Desde seu surgimento, as redes sem fio vêm ganhando espaços cada vez maiores, tanto na área industrial e comercial quanto no uso doméstico. Isso se deve, muitas vezes, ao seu menor custo de implantação, rápida instalação e capacidade de o usuário poder se deslocar sem perder acesso à rede. Entretanto, essas facilidades vêm associadas a dúvidas em relação à segurança dos dados.

Wrightson (2014) traz diversos princípios a respeito da segurança de sistemas em geral, e tais princípios se aplicam à segurança das redes sem fio independentemente do tipo de comunicação e/ou tecnologia que está atrelada a elas. O Quadro 3 apresenta, de maneira resumida, esses importantes princípios de segurança, que servirão de base para todos que desejam trabalhar na área de segurança da comunicação.

Quadro 3. Os 11 princípios para segurança

Princípio	Descrição
Segurança *versus* conveniência	Uma maior segurança é acompanhada de maior inconveniência. Por exemplo, a inclusão de senhas que expiram em determinados períodos de tempo para acesso à rede.
Não é possível eliminar todos os riscos	Para cada problema de segurança existem soluções que diminuem a chance de a brecha ser explorada. Porém não existe solução capaz de eliminar o risco totalmente.
Regras para o cálculo do risco	Existem diversas fórmulas para mensurarmos o risco de um problema. A mais usual é a seguinte expressão: Risco = Consequência × Probabilidade É comum realizarmos o cálculo do risco de diversos possíveis problemas de uma rede e apresentá-lo em uma matriz de riscos, como a apresentada na Figura 3.
Nem todo risco precisa ser eliminado	Muitos problemas associados à segurança não precisarão ser eliminados. Ao explorar a matriz de risco, podemos nos deparar com situações em que o risco e o dano causado por uma falha na segurança são pequenos, enquanto o custo para sanar o problema torna a operação impraticável.
Segurança não é só impedir pessoas não autorizadas	Existem diversas situações em que falhas na segurança e comprometimentos de dados críticos para a empresa são feitos por usuários com permissões de acesso à rede. Esse comprometimento dos dados pode ser causado por acidentes ou por falta de instrução em práticas de segurança por parte dos usuários.
Retorno de investimento não funciona para a segurança	O modelo de retorno de investimento aplicado por empresas não se aplica à segurança das redes, uma vez que aumentar a segurança da rede não irá retornar um montante à empresa. Esse aumento da segurança só irá impedir que danos possam ser causados.

(Continua)

(Continuação)

Quadro 3. Os 11 princípios para segurança

Princípio	Descrição
Defesa em profundidade	Um verdadeiro sistema de segurança não é construído com apenas uma medida de mitigação dos danos, mas por diversos sistemas que buscam soluções de maneiras inteligentes e eficazes.
Menores privilégios	Um método que pode facilmente aumentar a segurança da rede é o de dar aos usuários o menor número de privilégios e acessos à rede que permitam executar suas tarefas. Isso contrasta com a política comum de entregar todos os privilégios ao usuário e ir retirando privilégios perigosos um por um.
Confidencialidade, integridade e disponibilidade	Este é um conceito adotado pela indústria para sistemas de segurança, nos quais cada um dos pilares é vital para a segurança dos dados. ■ **Confidencialidade:** impede o acesso de pessoas não autorizadas aos dados. ■ **Integridade:** garante que modificações nos dados só possam ser feitas em situações e por pessoas autorizadas. ■ **Disponibilidade:** disponibiliza os dados na hora que solicitados, mantendo o fluxo de trabalho.
Prevenção, detecção e obstáculos	A maioria dos sistemas de segurança falha em uma destas categorias, de modo que é necessário implementar diversas estratégias de segurança para obter todos estes conceitos. ■ **Prevenção:** implementada para impedir que determinado problema ocorra. ■ **Detecção:** utilizada para detectar os pontos fracos da rede ou as atividades não permitidas na rede. ■ **Obstáculos:** impedem os usuários de fazerem algo que não deveriam.
Prevenção falha	Toda prevenção adotada irá, em algum momento, falhar ou é passível de falha.

Fonte: Adaptado de Wrightson (2014).

Outros conceitos importantes que permeiam a área de segurança de sistemas dizem respeito à autenticação e associação dos usuários e à encriptação dos dados. A associação e autenticação são quesitos importantes para o acesso do usuário de determinada rede. A **associação** a uma rede implica que o usuário e o ponto de acesso concordam com determinados parâmetros estabelecidos para a comunicação; já a **autenticação** é realizada para verificar se os usuários são autorizados a se comunicar com a rede. A **encriptação dos dados** funciona como nas demais tecnologias, nas quais os dados são codificados de modo que somente o destinatário e as pessoas autorizadas tenham acesso à informação como um todo.

Acompanhe a matriz de riscos na Figura 3.

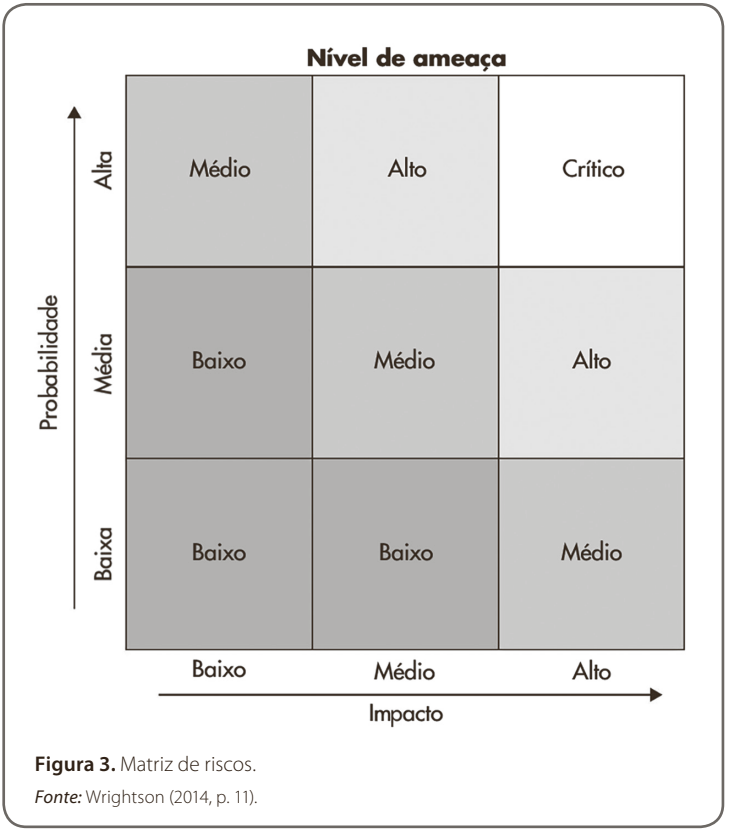

Figura 3. Matriz de riscos.
Fonte: Wrightson (2014, p. 11).

Nesta seção você estudou os princípios da segurança em redes sem fio. Esses princípios são fundamentais para o desenvolvimento do profissional que irá ingressar na área de segurança em redes sem fio. Na próxima seção, você verá um pouco mais sobre os diferentes dispositivos presentes nessas redes e o papel que esses aparelhos desempenham.

3 Equipamentos e dispositivos

Até agora foram apresentadas as características principais das redes sem fio, bem como discutidos os princípios relacionados à segurança desse tipo de tecnologia. Dessa forma, ainda precisamos ver os principais dispositivos e ferramentas que normalmente compõem a rede sem fio.

Fique atento

É especialmente importante estarmos atentos ao crescimento da tecnologia da **internet das coisas** (IoT, Internet of Things), que vem aumentando ainda mais o número de equipamentos capazes de se comunicar em uma rede sem fio.

Pontos de acesso

Este dispositivo vem se tornando cada vez mais popular com o crescimento das redes Wi-Fi. O ponto de acesso realiza a comunicação entre os diferentes dispositivos presentes na rede e os interliga a uma rede cabeada, servindo de acesso a rede maior, como a internet.

Este equipamento pode ser utilizado para, em conjunto, prover uma área de acesso maior, de modo a permitir que o acesso à rede não seja interrompido para usuários que estiverem em movimento. Outro ponto importante deste equipamento é que ele é responsável por implementar a segurança da comunicação entre os dispositivos presentes na rede (WRIGHTSON, 2014). No caso de redes Wi-Fi, por exemplo, temos os protocolos WPA (*Wi-Fi Protected Access*) e o WPA2 (*Wi-Fi Protected Access II*), considerados seguros na atualidade.

Smartphones

Presente no cotidiano de grande parte da população e indispensável nas mais diversas tarefas do dia a dia, o *smartphone* é um dispositivo cada dia mais presente. Talvez o melhor exemplo de dispositivo presente em redes sem fio, este equipamento combina as funções de computação e de celular em um único aparelho. Apresenta recursos de *hardware* e *software* mais potentes do que os encontrados em telefones convencionais, por isso é entregue um *software* abrangente, capaz de acessar a internet e a funcionalidade multimídia, além de ter as funções básicas de um telefone.

O *smartphone* ainda conta com um grande número de sensores, capazes de auxiliar o usuário em diversas tarefas. Além disso, este dispositivo dá suporte a diversos protocolos de comunicação sem fio, como *Bluetooth*, Wi-Fi e comunicação por satélite. Todas essas características impulsionaram o crescimento do mercado dos *smartphones*, que, em 2016, alcançou o número de 1,5 bilhões de unidades vendidas (MONGARDINI; RADZIKOWSKI, 2020).

Saiba mais

Se quiser saber mais sobre segurança para *smartphones*, o artigo "A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks" é uma boa leitura (em inglês). Ele trata dos principais desafios da atualidade, como vulnerabilidade do *software*, *malware* e ataques a estes dispositivos. Para encontrar este artigo, basta pesquisar pelo título em seu mecanismo de busca na internet.

Antenas

Outro equipamento bastante conhecido é a antena, que utiliza ondas de rádio para estabelecer a comunicação. Pode ser utilizada tanto para a transmissão quanto para a recepção de sinais. As antenas geralmente são projetadas para transmitir e receber ondas de rádio de uma direção particular, mas podem ser utilizadas em aplicações nas quais se deseja enviar ou receber um sinal por meio de direções horizontais.

Conforme Wrightson (2014), antenas apresentam os mais diversos tipos de estruturas e formatos. Porém, as mais comumente encontradas para fins de segurança são as omnidirecionais e direcionais. As **antenas direcionais** — ou setoriais, ou ainda Yagi —, como o próprio nome sugere, apresentam um caráter direcional, sendo apontadas para o transmissor de modo a elevar a potência do sinal e atingir maiores distâncias. **Antenas omnidirecionais** apresentam um espalhamento do sinal maior, propagando-o em todas as direções do plano horizontal da antena. Um exemplo da propagação do sinal emitido por essas antenas pode ser visto na Figura 4.

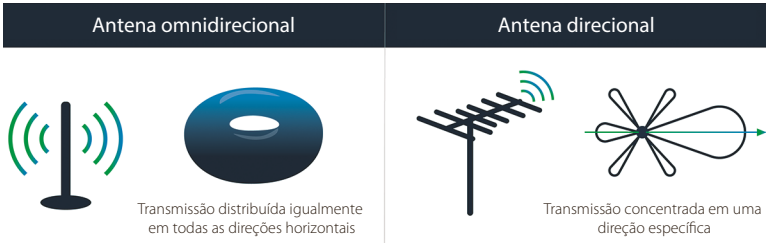

Figura 4. Antenas e a direção de transmissão.

Fonte: Behrtech (2020, documento *on-line*).

Satélites de comunicação

Estes dispositivos permitem a comunicação via satélite, na qual é criada uma comunicação entre fontes, transmitindo um sinal a fontes receptoras em locais normalmente separados por longas distâncias na Terra. Entre as aplicações deste tipo de equipamento estão o uso para redes telefônicas, televisão, rádio, acesso à internet e o uso por forças militares. A altitude do satélite geralmente determina a aplicação, com altitudes que podem chegar a 35.000km (TANENBAUM, 2003).

Dispositivos e a internet das coisas

Com o desenvolvimento da internet das coisas, o número de objetos capazes de se comunicar em redes sem fio vem crescendo rapidamente. Este é um conceito que estabelece a interconexão entre objetos presentes no nosso dia a dia, de modo que objetos que apresentem capacidade computacional se conectem à internet. Isso implica a possibilidade de objetos serem controlados e monitorados sem a interferência humana direta (TAN; WANG, 2010).

Esses conceitos abrem incontáveis possibilidades nos mais diversos setores, motivo pelo qual o profissional de redes sem fio terá um papel cada vez mais importante. Juntamente com o crescimento de novas tecnologias nas redes sem fio, surgem discussões ainda mais importantes referentes à segurança dessas redes. Com o aumento de objetos comunicando informações da rede e dos usuários em tempo real, será que a integridade das informações poderá ser mantida pelos métodos atuais de segurança?

A conexão dos dispositivos no conceito da internet das coisas utiliza sinais de rádio de baixa potência, de modo que esses sistemas poderiam se comunicar utilizando métodos diferentes dos já conhecidos Wi-Fi e *Bluetooth*.

Saiba mais

Para saber mais sobre internet das coisas e segurança, você pode ler o artigo "Current research on Internet of Things (IoT) security: A survey" (em inglês), que traz uma visão geral da segurança em sistemas com internet das coisas. Para complementar, a tese "Internet das coisas no Brasil: uma análise sobre propostas de conectividade e sua aderência aos atributos de segurança da informação" apresenta um estudo aprofundado e a revisão da literatura a respeito do plano de ação do BNDES para esta importante tecnologia. Para encontrar esses textos, basta pesquisar pelos títulos em seu mecanismo de busca na internet.

Neste capítulo, você estudou os conceitos fundamentais de redes sem fio. Ampliou o conhecimento sobre as vantagens desse tipo de rede em relação as já conhecidas redes cabeadas, bem como os tipos de comunicação utilizados nesse tipo rede. Também viu uma discussão sobre segurança das redes sem fio e os princípios de segurança que se aplicam a esses sistemas. Por fim, você conheceu um pouco mais sobre os diferentes dispositivos e ferramentas que estarão presentes no dia a dia do profissional da área de redes sem fio.

Referências

BEHRTECH. 6 *LPWAN antenna placement tips for optimal range*. [S. l.]: Behrtech, 2020. Disponível em: https://behrtech.com/blog/lpwan-antenna-placement/. Acesso em: 10 set. 2020.

KUROSE, J. F.; ROSS, K. W.; ZUCCHI, W. L. *Redes de computadores e a internet*: uma abordagem top-down. São Paulo: Pearson Addison Wesley, 2007.

MONGARDINI, J.; RADZIKOWSKI, A. *Global Smartphones Sales May Have Peaked*. Working Paper, n. 20/70, 2020. Disponível em: https://www.imf.org/en/Publications/WP/Issues/2020/05/29/Global-Smartphones-Sales-May-Have-Peaked--49361#:~:text=Summary%3A,market%20may%20now%20be%20saturated.. Acesso em: 10 set. 2020.

PASQUALINI, A. L.; MARCONDES, C. A. C. Estudo do crescimento das redes wireless 802.11–2.4 GHz em Ambiente Urbano–Caso Rio Claro-SP. *Revista TIS*, v. 1, n. 2, p. 167–175, 2012. Disponível em: http://revistatis.dc.ufscar.br/index.php/revista/article/viewFile/28/31. Acesso em: 10 set. 2020.

TAN, L.; WANG, N. *Future internet: the internet of things*. In: INTERNATIONAL CONFERENCE ON ADVANCED COMPUTER THEORY AND ENGINEERING (ICACTE), 3., 2010. Anais... [S. l.]: IEEE, 2010. p. V5-376–V5-380.

TANENBAUM, A. S. *Redes de computadores*. Rio de Janeiro: Campus, 2003.

WRIGHTSON, T. *Segurança de redes sem fio*: guia do iniciante. Porto Alegre: Bookman, 2014.

Leituras recomendadas

AHVANOOEY, M. T. et al. *A survey on smartphones security*: software vulnerabilities, malware, and attacks. International Journal of Advanced Computer Science and Applications, v. 8, n. 10, p. 2017, 2020.

BRANCO JÚNIOR, M. da R. *Internet das coisas no Brasil*: uma análise sobre propostas de conectividade e sua aderência aos atributos de segurança da informação. 2019. Dissertação (Mestrado em Sistemas de Informação e Gestão do Conhecimento)- Universidade Fumec, Belo Horizonte, 2019. Disponível em: https://repositorio.fumec.br/xmlui/bitstream/handle/123456789/421/manuel_%20Branco%20Junior_mes_sigc_2019.pdf?sequence=1&isAllowed=y. Acesso em: 10 set. 2020.

NOOR, M. B. M.; HASSAN, W. H. *Current research on Internet of Things (IoT) security*: a survey. Computer Networks, v. 148, p. 283–294, 2019.

Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

Conteúdo:

SAGAH
SOLUÇÕES EDUCACIONAIS INTEGRADAS