Alternatives for Data Protection in the Use of Wireless Networks Applied to Industry

Alternativas para a Proteção de Dados na Utilização das Redes sem Fio Aplicadas à Indústria

Ana Beatriz S. Nunes[1], Daniel Fabian C. Montoya[1], Thais Reggina Kempner[1]

[1]Faculdade de Engenharia de Várzea Grande -Univers. Federal de Mato Grosso(UFMT)
Av. Fernando Correa da Costa, nº 2367 - Boa Esperança. Cuiabá MT – CEP 78060-900
{ana.nunes, daniel.montoya}@sou.ufmt.br, thaisrgk@gmail.com

Abstract. *Wireless networks are increasingly present in the world's daily life and with each step that humanity advances in the digital age, its demand grows. This article aims to present a brief contextualization on the importance of using wireless networks in the industrial scenario, focusing on describing some methods that make them safer and more reliable, considering that the high risk linked to data protection is the biggest drawback of using the net. And ending with a challenging theme for the not so distant future, called: quantum cryptography.*
Keywords: *Wireless networks. Security. Quantum Cryptography. Data Protection. Industry.*

Resumo. *As redes sem fio estão cada vez mais presentes no cotidiano mundial e a cada passo que a humanidade avança na era digital, mais crescente é a sua demanda. O presente artigo tem por objetivo fazer uma breve contextualização sobre a importância da utilização das redes sem fio no cenário industrial, com foco em descrever alguns métodos que as tornem mais seguras e confiáveis, tendo em vista que o alto risco atrelado a proteção de dados é a maior desvantagem da utilização da rede. E encerra com um tema desafiador para um futuro não tão distante, denominado: criptografia quântica.*
Palavras-chave: *Redes sem fio. Segurança. Criptografia quântica. Proteção dos dados. Indústria.*

1. Introdução

No Brasil, a industrialização alavancou-se em meados de 1930, resultado da crise mundial de 1929, onde os produtos começaram a ser produzidos e comercializados localmente [Cano 2015]. Com o passar dos anos, houve uma evolução nítida nas indústrias e foi notório, o aumento da demanda de diferentes setores corporativos e uma necessidade de expansão industrial ainda maior para poder atendê-los [Viceconti 1977].

Recentemente, a Indústria 4.0 tem se estabelecido como o método e ferramenta mais presente na produção industrial. Máquinas, dispositivos, produtos e pessoas são conectados em tempo real por meio de tecnologias como redes de sensores sem fio, *big data*, computação em nuvem e sistemas embarcados [Santos, Volante 2018]. Em especial, a tecnologia de rede sem fio é essencial para a Indústria 4.0 pois aprimora significativamente a capacidade das empresas de se manterem competitivas em um ambiente de produção cada vez mais complexo e globalizado [Guerra 2020].

À medida que as redes sem fio se tornam cada vez mais presentes na vida cotidiana, torna-se mais crítica a necessidade de segurança. Qualquer indústria engajada em atividades com este tipo de rede, deve avaliar e gerenciar os riscos associados a estas práticas [Burnett, Steven 2002]. A utilização eficaz de técnicas criptográficas como a criptografia simétrica, a esteganografia e a criptografia quântica estão no núcleo de várias dessas estratégias de gerenciamento.

Nesse contexto, é importante utilizar tecnologias criptográficas para todas as operações que envolvam transmissão de dados sensíveis na indústria [Stallings 2008]. A utilização da criptografia de redes se mostra como uma solução efetiva a ser aplicada nas redes sem fio para garantir a confidencialidade, integridade e autenticidade dos dados transmitidos, bem como para proteger contra uma variedade de ameaças à segurança. Portanto, o objetivo desse trabalho é fazer uma breve contextualização sobre esse tipo de rede e descrever alguns métodos relacionados à segurança e à proteção dos dados transmitidos para tornar sua utilização mais segura e confiável.

2. As redes sem fio

O desenvolvimento das redes sem fio se remonta ao final do século XIX, com os experimentos em transmissão de ondas de rádio pelo físico italiano Guglielmo Marconi. culminando na primeira transmissão transatlântica sem fio em 1901 [Sarkar *et al*. 2006]. Só foi em 1940 que o exército americano aplicou essa tecnologia industrialmente.

Também conhecidas como *wireless networks*, as redes sem fio caracterizam todo tipo de redes de transmissão de informações que não utilizam cabos físicos para comunicação de dados. Em vez disso, as redes sem fio (*wifi, bluetooth*, conexão via satélite, dentre outras), utilizam ondas de rádio, infravermelho ou outros meios de comunicação sem fio para conectar dispositivos e transmitir mensagens com a mesma eficácia das redes convencionais cabeadas. Além disso, são de fácil instalação, alta confiança e flexibilidade, podendo operar no setor industrial, desde o chão de fábrica até o setor administrativo [Guerra 2020]. As redes sem fio seguem padrões específicos a depender da sua aplicabilidade:

- *Wireless Area Network* (WLAN): Baseadas no padrão IEEE 802.11 e variações.
- *Wireless Personal Area Network* (WPAN): padrão IEEE 802.15 e variações.
- *Wireless Wide Area Network* (WWAN): Baseadas no padrão IEEE 802.20.
- *Wireless Metropolitan Area Network* (WMAN): padrão IEEE 802.16.

As desvantagens das redes sem fio são o alto custo de implementação, a ausência de padronização no protocolo de comunicação dos equipamentos, e principalmente a segurança e privacidade dos dados. Portanto, a implementação de medidas de segurança adequadas, como criptografia de dados, é essencial para mitigar os riscos associados à utilização dessas redes na indústria.

3. Proteção de dados

A proteção das redes é um assunto que está sendo abordado há pelo menos três décadas. Em 1994 foi desenvolvido um relatório pelo *Internet Architecture Board* (IAB) com o

intuito de frisar a necessidade de mais proteção para os usuários da internet e apontar quais áreas de mecanismos estavam mais suscetíveis à invasão [Stallings , 2008].

Algumas das principais áreas a serem protegidas nas redes sem fio são: integridade, autenticidade, confidencialidade e disponibilidade das redes. Integridade é a garantia da não modificação (de nenhuma espécie) de uma mensagem durante sua transmissão. Na autenticidade temos mecanismos de verificação de mensagens de maneira a confirmar que o remetente é quem diz ser. A confidencialidade são mecanismos de proteção de uma mensagem de forma que usuários não autorizados não possam ter acesso a ela. A disponibilidade é a garantia de que o sistema vai estar sempre acessível evitando, principalmente, ataques de negação de serviço [Moraes, 2010].

A cada dia aumentam e se fazem mais sofisticados os ataques cibernéticos a dados na rede, sendo necessário menos conhecimento para causar mais danos. Por isso, foram desenvolvidos algoritmos base para proteção de dados. Quando uma mensagem deve ser enviada de um dispositivo para outro, por algum tipo de inter-rede, as duas partes devem contribuir para que isso ocorra; um canal de informação define uma rota para tal ação e então é acionada a proteção de dados. Uma informação secreta é usada junto com o algoritmo desenvolvido e um protocolo une o algoritmo à informação secreta, para que isso seja aplicado à rede [Stallings, 2008]. Introduz-se o conceito de criptografia, uma solução contra invasões na rede, seu funcionamento está descrito a seguir.

4. Criptografia de dados

A criptografia ou cifragem é um sistema que foi desenvolvido com a finalidade de dar proteção na conversão de um texto denominado “claro” (ou *plaintext*) para um texto cifrado (ou *ciphertext*). Existem pelo menos três tipos de criptografia mais usuais nos dias de hoje, a criptografia simétrica ou convencional, a assimétrica e a esteganografia. A criptografia necessita de um algoritmo combinado a uma chave secreta para criptografar e descriptografar uma mensagem enviada ou recebida. Existem três classificações para os sistemas criptográficos baseados em parâmetros distintos: Classificação por tipo de operação: substituição e transposição; Classificação por número de chaves utilizadas: únicas e diferentes; e Classificação por modo de processamento claro: cifra de bloco e cifra de fluxo.

O objetivo da criptografia é, manter a integridade da mensagem, e assegurar que durante o processo de substituição (quando o algoritmo faz a troca de um elemento no texto claro para que este fique “mascarado”) e de transposição (quando os elementos “mascarados” ficam de forma clara novamente), sejam mantidos todos os dados. [Stallings, 2008]. A criptografia, não é muito complexa na sua aplicação.

4.1. Criptografia Simétrica

Os algoritmos de criptografia simétrica utilizam uma chave secreta única para esconder e para decifrar um texto, não é preciso se preocupar com a proteção do algoritmo utilizado pois o que assegura a veracidade e integridade da mensagem é a chave secreta, que é diferente para cada usuário, [Stallings, 2008]. Aplicativos de troca de mensagens utilizam este método, uma chave secreta é desenvolvida cada vez que uma mensagem é enviada entre usuários, se houver a tentativa de utilizar uma chave no lugar da outra, a mesma não funcionará. Sem a chave a chance de ocorrer uma invasão é mínima, pois o algoritmo não consegue descriptografar o *ciphertext*.

4.2. Criptografia Assimétrica

Também chamada de criptografia de chave pública, oferece uma solução eficaz para garantir a confidencialidade, autenticidade e integridade dos dados, permitindo a comunicação segura em um ambiente digital. A criptografia assimétrica é uma técnica de criptografia que utiliza um par de chaves diferentes para cifrar e decifrar informações. Esse par de chaves consiste em uma chave pública e uma chave privada. A chave pública verifica o envio de uma mensagem com a ajuda de uma chave privada, e encriptação, só o portador da chave privada parelhada pode decriptar a mensagem com a chave pública. Já a chave privada é usada para decifrar mensagens ou dados que foram criptografados com a chave pública correspondente, ela é fundamental para garantir a autenticidade e a integridade dos dados, uma vez que somente o proprietário da chave privada pode decifrar as mensagens e verificar a autenticidade do remetente.

4.3. Esteganografia

A esteganografia é a prática de ocultar dados, usada para esconder mensagens dentro de outras mensagens. Essa técnica protege informações importantes e privadas, assegurando que apenas o destinatário adequado possa descobrir o conteúdo oculto. Sua origem remonta às regiões da Mesopotâmia por volta de 3500 a.C., e sua popularidade foi impulsionada pelos relatos de Johannes Trithemius [Mezzari 2012]. Termos importantes associados a essa prática incluem "*Cover Work*", uma imagem vazia que ainda não contém uma mensagem oculta, "*Stego-mensagem*", que é a mensagem oculta, "*Stego Work*", uma imagem preenchida contendo uma mensagem oculta, "*Estegograma*", uma mensagem com outra mensagem oculta transportada de forma que a mensagem original não seja percebida, e "*Estegosistema*", o sistema de esteganografia que permite o transporte da mensagem até o destinatário.

Essa técnica envolve usar uma "*Cover Work*" para transportar uma "*Stego mensagem*", transformando assim a antiga "*Cover Work*" em "*Stego Work*". Como um enigma, métodos são necessários para revelar a mensagem. Na era moderna, a esteganografia é implementada computacionalmente, permitindo que códigos sejam inseridos por trás de imagens JPEG, GIF ou até mesmo no domínio dos pixels. Algoritmos são necessários para a incorporação e extração desses códigos.

4.4. Criptografia Quântica

Tem como fundamento o desenvolvimento de computadores quânticos com processamento superior aos computadores tradicionais. Também conhecida como “distribuição quântica de chaves”, foi pauta na década dos 80 devido à abordagem por parte de Bennett e Brassard e pela influência de Richard Feynman. Bennett e Brassard, criaram o protocolo BB84 [Piqueira 2011], no qual é feita uma troca de mensagens a distância, por meio de uma sequência de bits enviados e decifrados através de fótons, os quais não permitem a cópia de um estado quântico. [Rigolin, Riesnik 2005].

A criptografia quântica é interessante para ser aplicada na segurança de redes sem fio por possuir particularidades que a tornam impossível de ser invadida. Uma delas é a capacidade de não permitir a cópia de um estado quântico (*non-cloning theorem*) e a outra se refere ao entrelaçamento de estados quânticos (*Quantic states entanglement*). A criptografia quântica existe no mercado, com muitas limitações e um custo muito elevado, porém, com indícios de que ganhará cada vez mais espaço, deixando a criptografia convencional totalmente ultrapassada.

6. Conclusões

Conhecer os métodos em criptografia de redes sem fio atualmente utilizados assim como os métodos em desenvolvimento e também aplicá-los de maneira integral na indústria é fundamental para trazer a segurança desejada pelos usuários e para continuar desenvolvendo e melhorando ainda mais as tecnologias na área.

É ideal que este conhecimento não se limite só aos desenvolvedores e encarregados das tecnologias de informação das corporações; todos os usuários que se beneficiam com o seu uso devem estabelecer boas práticas e aportar conhecimento e educação para as novas gerações de usuários que estarão cada vez mais ligados às redes com ou sem fio.

Referências

Burnett S., Steven B. (2002). Criptografia e segurança: O guia oficial RSA. *Gulf Professional Publishing*, Editora Campus, p. 367.

Cano, Wilson. Crise e industrialização no Brasil entre 1929 e 1954: A reconstrução do Estado Nacionale a política nacional de desenvolvimento. (2015). *Brazilian Journal of Political Economy*, v. 35, p. 444-460, 2015.

Moraes, Alexandre Fernandes. (2010) Redes sem fio: Instalação, Configuração e Segurança-Fundamentos. Saraiva Educação SA.

Guerra, A. R. (2020). Redes sem fio. Editora Contentus, Curitiba, p. 91. ISBN 978-65-5745-472-5.

Mezzari, Rafael. Utilização de esteganografia para ampliar confidencialidade em sistemas RFID. (2012). Dissertação de mestrado – Ciência da Computação, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre.

Piqueira, José Roberto C. (2011). Teoria quântica da informação: impossibilidade de cópia, entrelaçamento e teletransporte. *Revista Brasileira de Ensino de Física*, v. 33, n. 4, 4303.

Rigolin, G., Rieznik, A. A. (2005). Introdução à criptografia quântica. Revista Brasileira de Ensino de Física. *Revista Brasileira de Ensino de Física*, v. 27, n. 4., p. 215-526.

Santos, D. R. G.; Volante, C. R. (2018). A importância da tecnologia sem fio na Indústria 4.0. *Revista Interface Tecnológica*, v. 15, n. 2, p. 245-254. DOI: https://doi.org/10.31510/infa.v15i2.487

Sarkar, T. K., Mailloux R. J., Oliner, A. A., Salazar-Palma, M., Sengupta, D. (2006). History of wireless. John Wiley & Sons, p.660. DOI:10.1002/0471783021.

Stallings, William (2008). Criptografia e segurança de redes: princípios e práticas. 4. ed. P. 492 São Paulo: Pearson Education do Brasil. Xvii. ISBN:9788576051190.

Viceconti, P. E. (1977). O processo de industrialização brasileira, p. 33-43 2012. Disponível em: https://www.scielo.br/j/rae/a/jXTDXVDgshvB4PZdYxfqHkN/?lang=pt&format=pdf Acesso em: setembro. 2023.