Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v11i12.22900

PROTOCOLOS DE SEGURANÇA PARA INTERNET DAS COISAS (IOT)

SECURITY PROTOCOLS FOR THE INTERNET OF THINGS (IOT)

PROTOCOLOS DE SEGURIDAD PARA EL INTERNET DE LAS COISAS (IOT)

Ítalo Rodrigo Monte Soares[1]
Saylon Ferreira Alencar[2]

RESUMO: A Internet das Coisas (IoT) tem se proliferado de maneira ágil em diferentes segmentos, interligando dispositivos utilizados em residências, indústrias, áreas urbanas e na saúde. Entretanto, essa extensa conectividade traz à tona desafios consideráveis relacionados à segurança da informação, sobretudo em virtude das restrições de processamento, memória e consumo de energia dos dispositivos de Internet das Coisas (IoT). O presente artigo visa examinar os principais protocolos de segurança implementados na Internet das Coisas (IoT), além de avaliar as vulnerabilidades existentes nos protocolos de comunicação mais comuns, como MQTT, CoAP e AMQP. A metodologia utilizada fundamenta-se em uma revisão bibliográfica de artigos científicos veiculados entre 2020 e 2025 em bases de dados como IEEE, *Springer*, *Science Direct* e revistas nacionais. Os resultados da revisão mostram que, apesar da existência de mecanismos como TLS/DTLS, criptografia de nível e modelos de autenticação, diversos protocolos continuam a confiar em soluções externas para segurança, revelando vulnerabilidades relativas à confidencialidade, integridade e autenticação das informações. à conclusão de que a segurança na Internet das Coisas (IoT) exige estratégias específicas, incluindo protocolos otimizados e desenvolvidos dentro da lógica de "segurança por design", bem como a implementação de práticas constantes de atualização e monitoramento. A pesquisa também identifica deficiências e possíveis futuras, evidenciando a urgência de normatização e de protocolos mais eficazes para equipamentos de baixa capacidade.

Palavras-chave: Internet das Coisas. Protocolos de Segurança. Cibersegurança.

ABSTRACT: The Internet of Things (IoT) has rapidly proliferated across various sectors, interconnecting devices used in homes, industries, urban areas, and healthcare. However, this extensive connectivity raises considerable challenges related to information security, especially due to the processing, memory, and energy consumption limitations of IoT devices. This article aims to examine the main security protocols implemented in the Internet of Things (IoT), as well as evaluate the vulnerabilities in the most common communication protocols, such as MQTT, CoAP, and AMQP. The methodology used is based on a literature review of scientific articles published between 2020 and 2025 in databases such as IEEE, Springer, Science Direct, and national journals. The results of the review show that, despite the existence of mechanisms such as TLS/DTLS, layer-level encryption, and authentication models, several protocols continue to rely on external solutions for security, revealing vulnerabilities related to the confidentiality, integrity, and authentication of information. The research concludes that security in the Internet of Things (IoT) requires specific strategies, including optimized protocols developed within the logic of "security by design," as well as the implementation of constant updating and monitoring practices. The research also identifies deficiencies and potential future problems, highlighting the urgency of standardization and more effective protocols for low-capacity equipment.

Keywords: Internet of Things. Security Protocols. Cybersecurity.

[1]Mestre em Engenharia Elétrica, Universidade Federal de Campina Grande.
[2]Professor. orientador na UNIFSA – Centro Universitário Santo Agostinho.
Acadêmico de Graduação do Curso de Bacharelado em Engenharia Elétrica na UNIFSA – Centro Universitário Santo Agostinho, Teresina – PI.

RESUMEN: El Internet de las Cosas (IoT) se ha extendido rápidamente por diversos sectores, interconectando dispositivos utilizados en hogares, industrias, áreas urbanas y el ámbito sanitario. Sin embargo, esta amplia conectividad plantea importantes desafíos relacionados con la seguridad de la información, especialmente debido a las limitaciones de procesamiento, memoria y consumo energético de los dispositivos IoT. Este artículo examina los principales protocolos de seguridad implementados en el Internet de las Cosas (IoT), así como evalúa las vulnerabilidades de los protocolos de comunicación más comunes, como MQTT, CoAP y AMQP. La metodología empleada se basa en una revisión bibliográfica de artículos científicos publicados entre 2020 y 2025 en bases de datos como IEEE, Springer, Science Direct y revistas nacionales. Los resultados de la revisión muestran que, a pesar de la existencia de mecanismos como TLS/DTLS, cifrado por capas y modelos de autenticación, varios protocolos siguen dependiendo de soluciones externas para la seguridad, lo que revela vulnerabilidades relacionadas con la confidencialidad, la integridad y la autenticación de la información. La investigación concluye que la seguridad en el Internet de las Cosas (IoT) requiere estrategias específicas, incluyendo protocolos optimizados desarrollados bajo la lógica de "seguridad por diseño", así como la implementación de prácticas de actualización y monitoreo constantes. El estudio también identifica deficiencias y posibles problemas futuros, destacando la urgencia de la estandarización y de protocolos más efectivos para equipos de baja capacidad.

Palabras clave: Internet de las cosas. Protocolos de seguridad. Ciberseguridad.

INTRODUÇÃO

Nos últimos anos, a Internet das Coisas (*Internet of Things* – IoT) firmou-se como uma das tecnologias mais revolucionárias e cruciais para o progresso da sociedade interconectada. A proposta fundamental consiste na integração de elementos físicos ao universo digital através de sensores, atuadores, redes sem fio e plataformas inteligentes, possibilitando que dispositivos de diversas categorias coletem, processem, compartilhem e transmitam informações em tempo real. Essa integração tem mudanças significativas em áreas como saúde, indústria, mudanças, transporte, logística, educação, segurança pública e no âmbito residencial, resultando em uma maior eficiência operacional, automação e comodidade para os usuários.

No entanto, o rápido crescimento do ecossistema IoT não acontece sem obstáculos. O crescimento exponencial da quantidade de dispositivos conectados — estimado em bilhões em todo o mundo — expõe vulnerabilidades que podem afetar a privacidade, a integridade e a disponibilidade de sistemas inteiros. Ao contrário dos computadores convencionais, os dispositivos de IoT costumam ter uma arquitetura limitada, com capacidade de processamento e memória reduzida, baixo consumo de energia e utilização de protocolos de comunicação níveis. Como resultado, muitos desses dispositivos funcionam com mecanismos de segurança inadequados ou ausentes, tornando-se alvos vulneráveis para invasores.

A heterogeneidade característica da IoT torna o cenário ainda mais complexo. Em um ambiente onde geralmente não existe uma padronização consolidada, diversos fabricantes, sistemas operacionais, padrões de comunicação e topologias de rede coexistem. Essa a fragmentação torna mais difícil a aplicação de mecanismos de consistentes e interoperáveis, gerando brechas que podem afetar a segurança de toda a arquitetura. Além disso, muitos aparelhos são criados com baixo custo e agilidade na colocação no mercado, o que, na prática, leva à negligência dos requisitos básicos de segurança, como autenticação, criptografia sólida ou atualização de *firmware*.

Nesse cenário, os protocolos de segurança para IoT são destacados como essenciais para garantir um nível básico de proteção em ambientes interconectados. Esses Os protocolos têm a função de definir diretrizes e ferramentas que permitem à autenticação de dispositivos, a criptografia das comunicações, a integridade dos dados enviados e a proteção contra ataques cibernéticos. No entanto, criar protocolos eficazes para IoT não é uma tarefa simples: além das restrições técnicas dos dispositivos, é preciso equilibrar desempenho, consumo de energia, escalabilidade e custo, garantindo que os mecanismos de segurança não comprometam a operação dos aparelhos.

Entre os protocolos de comunicação mais usados na IoT — como MQTT, CoAP, AMQP, LoRaWAN e ZigBee — observa-se que a maior parte foi desenvolvida com ênfase na leveza e eficiência, e não, necessariamente, na segurança. Portanto, para atingir níveis adequados de segurança, eles dependem de camadas externas, como TLS/DTLS ou criptografia adicional. Esse O caso mostra que muitos protocolos IoT não disponibilizam, de forma nativa, mecanismos de defesa avançados, transferindo uma grande parte da responsabilidade de segurança para administradores, desenvolvedores e arquitetos de rede.

Por consequência, falhas em protocolos e implementações têm sido exploradas com frequência. Nos últimos anos, houve vários ataques que receberam atenção internacional, incluindo a formação de *botnets* feitos com dispositivos IoT comprometidos, ataques DDoS (negação de serviço distribuído), interceptação de mensagens, falsificação de comandos, bem como invasões a câmeras, roteadores, sensores industriais e dispositivos domésticos. Esses eventos demonstram que, na ausência de protocolos de segurança robustos, o ecossistema IoT se transforma em um terreno fértil para falhas graves, colocando em risco não apenas usuários individuais, mas também infraestruturas críticas, como redes hospitalares, sistemas de energia e centros de monitoramento das cidades.

As dificuldades também se prolongam por toda a duração dos ciclos de vida dos dispositivos da Internet das Coisas. Diversos dispositivos continuam em funcionamento durante anos, sem receber as devidas atualizações de segurança, seja em virtude de restrições técnicas, falta de assistência do fabricante ou falta de conhecimento por parte do usuário. Demais são instalados em locais de difícil acesso físico, o que torna inviável a manutenção frequente. Em inúmeras situações, ao serem identificadas como vulnerabilidades, não há um sistema de atualização remota (*over-the-air*), ou que prolongam as deficiências e aumentam a chance de exploração maliciosa.

Diante desse cenário, torna- se claro o imperativo de expandir a pesquisa sobre protocolos de segurança direcionados ao ecossistema da Internet das Coisas direcionados ao ecossistema da Internet das Coisas (IoT). A comunidade acadêmica e a indústria têm progredido em investigações externas para o aprimoramento de criptografia leve, protocolos de comunicação seguros, modelos de autenticação otimizados, detecção inteligente de intrusões e abordagens de segurança fundamentadas em aprendizado de máquina. Contudo, persiste uma extensa trajetória a ser trilhada, particularmente no que diz respeito à normalização global, à interoperabilidade e à adequação dos protocolos à realidade de dispositivos altamente restritos.

Diante desse contexto, o presente artigo busca investigar os principais protocolos de segurança empregados na Internet das Coisas, enfatizando suas particularidades, aplicações, restrições e desafios. Além disso, procure abordar as vulnerabilidades comumente encontradas em protocolos de comunicação amplamente utilizados, como MQTT, CoAP e AMQP, destacando de que maneiras essas fragilidades podem capacitar todo o ecossistema da Internet das Coisas (IoT). A partir dessa avaliação, busca-se evidenciar a relevância das estruturas de segurança sólidas, da aplicação de criptografia integrada e da adoção de práticas contemporâneas de proteção cibernética.

Nesse sentido, efetua-se uma revisão bibliográfica fundamentada em pesquisas divulgadas entre 2020 e 2025, englobando artigos indexados em repositórios científicos como IEEE *Xplore, SpringerLink, ScienceDirect,* Google Scholar e revistas acadêmicas brasileiras. A escolha de publicações contemporâneas possibilita a compreensão da progressão das investigações no campo, além de permitir a identificação de tendências tecnológicas e desafios contínuos. Essa estratégia permite, além disso, realizar comparações entre soluções, identificar lacunas e elaborar recomendações para a adoção de medidas de segurança mais eficientes em ambientes de Internet das Coisas (IoT).

A importância desta pesquisa é fundamental no cenário atual, no qual a Internet das Coisas (IoT) se incorpora progressivamente às práticas sociais e produtivas. Na ausência de mecanismos de segurança, os dispositivos conectados podem tornar-se vetores para ataques que comprometam não apenas dados pessoais, mas também a operação integral de redes corporativas, industriais e governamentais. Dessa forma, entender os protocolos de segurança pertinentes à Internet das Coisas (IoT) é fundamental para fomentar a criação de ambientes interconectados mais seguros, resilientes e capacitados para lidar com as ameaças digitais vindas.

Nesse contexto, a segurança deve ser considerada não como uma fase adicional, mas como um componente essencial no desenvolvimento de dispositivos e soluções de Internet das Coisas (IoT). A implementação da filosofia "*security by design*" — ou segurança desde a concepção— revela-se essencial para garantir que as tecnologias inovadoras sejam cumpridas de maneira responsável e sustentável. Dessa forma, protocolos de segurança eficazes e corretamente implementados exercem uma função fundamental, uma vez que especificamente o alicerce que garante a comunicação segura entre dispositivos, usuários, plataformas e serviços digitais.

Assim, ao analisar os protocolos de segurança mais relevantes para a Internet das Coisas (IoT), este artigo oferece uma contribuição significativa para o enriquecimento do debate acadêmico e tecnológico acerca do tema, auxiliando profissionais, pesquisadores e estudantes na compreensão dos riscos, desafios e soluções potenciais para a proteção de sistemas interconectados. No entanto, pretende-se que esta análise funcione como um referencial para investigações futuras e para a melhoria das práticas de segurança em contextos cada vez mais condicionados por dispositivos inteligentes.

CONCEITO E REQUISITOS DE SEGURANÇA EM IOT

A Internet das Coisas (IoT) constitui um dos fundamentos essenciais da transformação digital atual, sendo definida pela habilidade de interligar objetos físicos, sensores, atuadores, veículos, máquinas e dispositivos embutidos por meio de redes sem fio e plataformas inteligentes. A interconectividade mencionada viabiliza a coleta ininterrupta de dados, e a de fundamentadas em informações em decisões em tempo real, alterando de maneira significativa os contextos domésticos, industriais e urbanos. Entretanto, essa ampla expansão acarreta desafios substanciais no âmbito da segurança da informação, dado que diversos dispositivos de

Internet das Coisas (IoT) funcionam com restrições de capacidade computacional, memória escassa e compatibilidade reduzida com protocolos de criptografia complexos. Tal limitação afeta diretamente a execução de níveis de proteção sólida e gera uma área de ataque expandida, suscetível a comprometer sistemas completos quando vulnerabilidades são aproveitadas (Ramakrishnan *et al* ., 2020).

A diversidade estrutural da Internet das Coisas (IoT) — que abrange diversos fabricantes, sistemas operacionais, arquiteturas de hardware, padrões de comunicação e softwares embarcados — torna o ecossistema ainda mais suscetível a vulnerabilidades, complicando a uniformização de mecanismos de segurança. De acordo com uma pesquisa divulgada na Revista Intercursos da UEMG, a diversidade de dispositivos e a ausência de padronização nos protocolos impedem o desenvolvimento de soluções integradas, resultando na implementação de modelos de segurança que são inconsistentes e vulneráveis a falhas. A fragmentação tecnológica permite a ocorrência de ameaças como *spoofing*, sequestro de sessões, manipulação *de firmware* e expansão de senhas fornecidas, principalmente devido ao fato de que muitos dispositivos de Internet das Coisas (IoT) são comercializados com credenciais padrão, as quais são especificamente modificadas pelos usuários (Ferreira, 2022).

Outro aspecto preocupante refere-se à falta de atualizações frequentes de *firmware*, uma prática fundamental para a correção de falhas de segurança. Em dispositivos de Internet das Coisas (IoT), a atualização de atualização pode se tornar técnico inviável, seja pela ausência de suporte por parte do fabricante, ou pela inexistência de mecanismos seguros para atualizações *over-the-air* (OTA). Publicações na A *Science Direct* salienta que a ausência de um ciclo de manutenção sistemático converte dispositivos em fontes constantes de risco, possibilitando que vulnerabilidades já conhecidas sejam exploradas por períodos prolongados. Além disso, numerosos dispositivos são posicionados em áreas de difícil acesso, o que torna ainda mais intricada a tarefa de corrigir falhas e renovar certificados digitais (Anand *et al*., 2022).

A literatura acadêmica demonstra que a maior parte dos ataques direcionados à Internet das Coisas (IoT) explora vulnerabilidades fundamentais relacionadas à comunicação e à autenticação. Protocolos amplamente utilizados, como MQTT e CoAP, foram desenvolvidos para garantir nível, eficiência energia e reduzido consumo de largura de banda, priorizando o desempenho em relação à segurança específica. Estudos altamente reconhecidos no âmbito internacional, incluindo os divulgados pela Springer, evidenciaram que o MQTT não incorpora mecanismos internos de criptografia robustos, dependendo unicamente de camadas

suplementares, como o TLS, para garantir a confidencialidade. Na ausência dessa camada, conforme informações circulam em texto simples, o que torna dados vulneráveis a interceptações e alterações maliciosas ataques do tipo *emin - the - middle* (AL - QAHTANI , 2020).

Para além dos riscos garantidos aos protocolos de comunicação, existem igualmente os desafios inerentes à autenticação e à administração de identidades nos ecossistemas da Internet das Coisas (IoT). Em diversas situações, aparelhos realizando conexões com servidores centrais, serviços em nuvem ou *gateways* locais, muitas vezes sem a necessidade de validação. Isso gera possibilidades para que indivíduos de má-fé insiram dispositivos falsificados ou controlem, de maneira remota, equipamentos comprometidos. Estudos divulgados na IEEE Xplore evidenciam que a falta de autenticação robusta e de criptografia apropriada possibilita o envenenamento de dados, a falsificação de permite o envenenamento de dados , a falsificação de pacotes e o controle inadequado de dispositivos essenciais, especialmente em pacotes e industriais e em infraestruturas urbanas delicadas (Singh et al., 2023).

A interação entre elementos de diversos fabricantes torna o contexto ainda mais complexo. Cada prestador de serviços adota suas próprias abordagens de comunicação, variações de protocolos e sistemas exclusivos, resultando em ambientes híbridos que apresentam dificuldades para serem padronizados. Pesquisas divulgadas pela A UEMG ressalta que, em redes disponíveis por numerosas ou centenas de dispositivos variados, a ausência de segurança incluída em apenas um componente pode colocar em risco toda a rede. Essa comunicação, denominado “ponto fraco sistêmico”, evidencia que a Internet das Coisas (IoT) funciona na premissa de que a segurança da rede é tão robusta quanto o seu dispositivo mais suscetível (Martins, 2021).

Um outro ponto amplamente abordado na literatura refere-se à constituição de *botnets* de Internet das Coisas (IoT), conforme evidenciado por vários ataques documentados desde 2016. Estudos indexados na Springer abordam como dispositivos convencionais — Órfãos câmeras IP, lâmpadas inteligentes, roteadores residenciais e sensores — são frequentemente integrados a redes zumbis, responsáveis por executar ataques distribuídos de negação de serviço (DDoS). Esses *botnets* exploram dispositivos que estão mal configurados e desatualizados para formar uma infraestrutura de grande escala, capaz de incapacitar sites, ”empresariais e plataformas digitais completas. Essa conjuntura evidencia a repercussão mundial da vulnerabilidade na Internet das Coisas, visto que um aparelho básico e de baixo custo pode

provocar estragos em nível global quando inserido em um ataque orquestrado (Wang *et al.*, 2020).

Finalmente, o princípio de "*security by design*" surge como uma das principais orientações de estudos, organismos internacionais e entidades acadêmicas. Proponho argumentar que a segurança não deve ser adicionada de forma tardia, como um adicional ao sistema, mas sim rompida desde as fases iniciais de concepção e desenvolvimento do dispositivo. Isso abrange a seleção prévia de protocolos seguros, a adoção de criptografia leve em conformidade com as limitações do *hardware*, a utilização de autenticação sólida, a implementação de mecanismos de atualização seguros e uma política definida para o ciclo de vida. Conforme artigos da *ScienceDirect*, uma criação de ecossistemas de A Internet das Coisas (IoT) que são resistentes, escaláveis e confiáveis ocorre somente quando os fabricantes assumem plena responsabilidade pelo projeto seguro (Kumar *et al.*, 2022).

PROTOCOLOS DE COMUNICAÇÃO E DESAFIOS DE SEGURANÇA EM IOT

Os protocolos de comunicação exercem uma função essencial na operação da Internet das Coisas, uma vez que são encarregados de estabelecer a conexão entre dispositivos físicos, servidores, plataformas em nuvem e sistemas de controle distribuído. Diferentemente das redes convencionais, nas quais se observa um elevado poder computacional e um tráfego de dados relativamente uniformizado, os ambientes de Internet das Coisas (IoT) exigem protocolos que sejam leves, eficientes e com baixo consumo de energia. Essa influência deve-se ao fato de que diversos dispositivos são concebidos para funcionar com baterias de tamanho reduzido, memória restrita e capacidade de processamento limitada. Conforme estudo divulgado na Springer, protocolos como MQTT, CoAP e AMQP emergiram para satisfazer a necessidade de eficiência e simplicidade; no entanto, foram originalmente planejados com ênfase na comunicação, ao invés de na segurança em si, o que resultou em lacunas que serão supridas por camadas extras de proteção (Al-Qahtani, 2020).

O protocolo MQTT (*Message Queuing Telemetry Transport*) destaca-se como um dos mais úteis em soluções de Internet das Coisas (IoT), em virtude de sua arquitetura fundamentada no modelo de publicação e subscrição (*publish/subscribe*), que possibilita uma comunicação eficiente, mesmo em redes com largura de banda restrita. Contudo, pesquisas indicam que o MQTT, em sua configuração original, não possui mecanismos eficazes de criptografia ou autenticação. Estudos publicados em periódicos Cientistas brasileiros

evidenciaram que, na ausência da implementação conjunta com TLS, as mensagens podem transitar em texto não criptografado, tornando-se vulneráveis a interceptações, manipulações e ataques *man-in-the-middle*. Além disso, diversos dispositivos empregam credenciais padrão ou autenticação básica, o que amplifica os riscos de invasão e sequestro de sessão. A literatura destaca que a leveza do MQTT é, ao mesmo tempo, sua característica mais positiva e sua principal fragilidade, uma vez que a falta de segurança interna exige configurações suplementares, muitas vezes ignoradas em implementações comerciais (Ferreira, 2022).

Um protocolo que é amplamente empregado na Internet das Coisas (IoT) é o CoAP (*Constrained Application Protocol*), que foi desenvolvido pela IETF, tendo como objetivo a comunicação com dispositivos limitados e fundamentada no modelo REST. O CoAP foi desenvolvido para funcionar com o protocolo UDP e, dessa forma, fornece baixa latência e agilidade na transmissão de dados em redes restritas. Entretanto, assim como o MQTT,o O CoAP requer camadas externas — notadamente o DTLS — para garantir uma comunicação segura. Além disso, dispositivos que empregam CoAP costumam funcionar em ambientes expostos, como no caso de sensores agrícolas ou industriais, ou que elevam a probabilidade de acessos não autorizados, caso a proteção criptográfica não seja especificamente aplicada (Anand *et al.*, 2022).

O AMQP (Protocolo Avançado de Filas de Mensagens), apesar de ser mais robusto do que o MQTT e o CoAP, também enfrentou dificuldades ao implementar dispositivos de IoT com recursos restritos. O protocolo é frequentemente empregado em sistemas empresariais de alto desempenho, mas também foi integrado a soluções de Internet das Coisas, principalmente em segmentos que exigem alta confiabilidade na transmissão e recepção de dados. Embora o AMQP incorpore mecanismos de segurança interna, como controle de fluxo e validação estruturada de mensagens, sua aplicação pode ser onerosa para dispositivos embarcados de baixo consumo. Em virtude disso, a implementação exige uma análise minuciosa sobre a capacidade computacional e energética dos dispositivos implicados, uma vez que sua complexidade pode afetar o desempenho e a autonomia (Wang *et al.*, 2020).

Além dos protocolos de aplicação, como tecnologias de comunicação de longa distância e com baixo consumo de energia também enfrentam desafios específicos relacionados à segurança. Redes como LoRaWAN, por sua vez, são amplamente utilizados em contextos industriais e em cidades inteligentes, pela razão de sua habilidade em transmitir dados a grandes distâncias com baixo consumo de energia. Dos avanços das versões mais recentes da tecnologia,

permanecem riscos relacionados ao uso impróprio de chaves criptográficas e à duplicação de pacotes, especialmente em contextos em que os dispositivos não são atualizados por longos períodos (Singh *et al.*, 2023).

Ao analisar a segurança dos protocolos de comunicação, evidencia-se que, na maioria das vezes, as vulnerabilidades não residem apenas nas tecnologias em si, mas na maneira como estas são inovadoras. A literatura ressalta que vários ataques ocorrem não por deficiências estruturais dos protocolos, mas em decorrência de configurações internas, de autenticação fraca e de falta de criptografia. As brasileiras divulgadas na Revista Intercursos indicam que, em muitas implementações de IoT, os dispositivos são interligados de forma apressada, sem a devida atenção pela segurança, o que abrange o uso de senhas padrão, portas abertas, falta de auditorias e a inexistência de mecanismos de segregação da rede, contexto que favorece a exploração de falhas de segurança e a propagação de ataques por toda a infraestrutura (Martins, 2021).

O aspecto crucial apontado pelas pesquisas é a complexidade da padronização entre diversos fabricantes, equipamentos que operam com protocolos distintos interagem em uma rede única, é habitual que *gateways* interfiram na tradução de protocolos, o que pode gerar novos vetores de ataque, principalmente se esses *gateways* não forem particularmente protegidos. Qualquer elemento intermediariamente ativado pode atuar como um vetor de ataque, principalmente empode atuar como um vetor de ataque, principalmente em topologias distribuídas ou em redes que empregam diversas camadas de roteamento (RAMAKRISHNAN et al., 2020) .

Na última análise, a dificuldade em atualizar o *firmware* configura-se como um dos principais obstáculos de segurança associados aos protocolos de comunicação. Ainda que os protocolos disponibilizam suporte à criptografia e à autenticação, a ausência de atualizações verifique a correção oportuna das vulnerabilidades identificadas. Dispositivos de Internet das Coisas (IoT) frequentemente operam por longos períodos com software desatualizado, possibilitando que ataques conhecidos sejam explorados de forma indefinida. Ainda mais preocupante, diversos dispositivos não são capazes de receber atualizações seguras via OTA, o que os torna permanentemente suscetíveis a ameaças que se acumulam ao longo do tempo (Kumar et al., 2022).

PROTOCOLOS DE SEGURANÇA PARA IOT: MECANISMOS, LIMITAÇÕES E TENDÊNCIAS

O desenvolvimento da Internet das Coisas exige a implementação de protocolos de segurança que garantam um funcionamento confiável de dispositivos, redes e plataformas, garantindo a proteção de dados e prevenção de transações prejudiciais. Considerando que diversos protocolos de comunicação empregados em IoT — como MQTT, CoAP e AMQP — carecem de segurança intrínseca, é necessária a utilização de protocolos dedicados à proteção, tais como TLS, DTLS, IPsec, criptografia leve e modelos avançados de autenticação. A Internet das Coisas (IoT) é condicionada por um conjunto de estratégias, abrangendo criptografia, autenticação , controle de acesso, integridade das mensagens e monitoramento constante. Assim, não reside apenas no protocolo utilizado, mas também na forma como esta segurança é configurada e integrada ao ecossistema de Internet das Coisas (IoT), levando em consideração as restrições de energia e processamento dos dispositivos interconectados (Al-Qahtani, 2020).

O TLS (*Transport Layer Security*) é amplamente empregado na proteção de protocolos de aplicação, notadamente em contextos de MQTT. Assegurar a confidencialidade e integridade através a utilização de criptografia assimétrica, autenticação por meio de certificados e a criação de sessões de maneira segura. Contudo, em virtude de sua complexidade computacional, a implementação em dispositivos de Internet das Coisas com recursos limitados pode resultar em sobrecarga energética e elevação da latência, comprometendo aplicações que são sensíveis ao tempo. Apesar de o TLS fornecer uma segurança sólida, sua aplicação em dispositivos com limitações não comsimples , exigindo otimizações ou a substituição por opções mais leves. Entretanto, essa continua sendo a solução mais empregada para garantir a segurança das comunicações entre dispositivos de Internet das Coisas (IoT) e servidores centrais, especialmente em contextos industriais, sociais e corporativos (Anand *et al.*, 2022).

O DTLS (*Datagram Transport Layer Security*) apresenta-se como uma alternativa ao TLS quando a comunicação é realizada por meio do UDP, como ocorre com o protocolo CoAP. Destinado para garantir a segurança em conexões instáveis ou suscetíveis à perda de pacotes — situação frequente em redes de Internet das Coisas (IoT) — o DTLS fornece criptografia, autenticação e proteção contra ataques de reprodução, preservando um desempenho adequado em dispositivos com recursos limitados. Entretanto, de maneira semelhante ao TLS, o DTLS também se depara com dificuldades vinculadas ao consumo de energia e à complexidade na sua implementação. Pesquisas divulgadas em palestras do IEEE indicam que o processo de

handshake do DTLS pode ser custoso em sistemas com recursos limitados de memória, o que prejudica a eficiência em aplicações que demandam alta frequência de troca de mensagens ou em dispositivos com capacidade reduzida de bateria (Singh *et al.*, 2023).

Outros mecanismos que têm sido amplamente examinados na literatura incluem o IPsec, gerenciador de redes fundamentadas em IP. Apesar de fornecer criptografia avançada, autenticação, integridade e a segurança de pacotes na camada de rede, o IPsec é classificado como oneroso para os ambientes tradicionais de Internet das Coisas (IoT). Embora o IPsec possuísse um elevado nível de segurança, ele requer uma capacidade específica de processamento e memória, o que o torna impróprio para dispositivos com limitações, a não ser que seja implementado exclusivamente em *gateways* ou equipamentos intermediários que disponham de maior capacidade computacional. A aplicação de sensores, atuadores e controladores embarcados frequentemente se mostra inviável em virtude do impacto direto que exerce sobre o consumo de energia e a autonomia do dispositivo (Wang *et al.*, 2020).

A criptografia leve constitui uma das principais inovações em segurança para a Internet das Coisas (IoT). Criado para espaços limitados, emprega algoritmos melhorados que diminuem o custo computacional, mantendo a segurança. Algoritmos de leves podem diminuir o consumo de energia em até 40% em relação às criptografias tradicionais, o que os torna adequados para dispositivos como sensores remotos, etiquetas inteligentes e câmeras com capacidade reduzida. Entretanto, os estudiosos alertam que a criptografia leve ainda não atinge o mesmo grau de maturidade e padronização das criptografias deliberadamente, exigindo avaliações rigorosas antes de ainda adoção em aplicações críticas, como saúde, energia ou transporte (Kumar *et al.*, 2022).

Um elemento fundamental para a segurança na Internet das Coisas (IoT) é a implementação de protocolos e mecanismos de autenticação, os quais garantem que somente dispositivos autorizados possam se conectar à rede. A literatura enfatiza que a falta de autenticação robusta figura como uma das principais razões para invasões e sequestros de dispositivos de Internet das Coisas (IoT). Um artigo publicado na Revista Intercursos enfatiza que diversas implantações recorrem unicamente à autenticação básica, o que torna mais simples a execução de ataques de falsificação de dispositivos e a interceptação de dados. Métodos mais sofisticados, como a autenticação fundamentada em certificados digitais ou chaves assimétricas, são recomendados; entretanto, requerem uma capacidade maior de memória e de processamento, o que dificulta sua implementação em dispositivos de custo extremamente

reduzido. Pesquisadores, hoje, argumentam que modelos de autenticação escalavam são fundamentais para prevenir ataques de personificação e manipulação de dados (Ferreira, 2022).

Além disso, os mecanismos de controle de acesso exercem uma função essencial na segurança dos sistemas de Internet das Coisas (IoT), principalmente em contextos industriais ou empresariais. O controle fundamentado em papéis (RBAC) e em atributos (ABAC) é amplamente desenvolvido em sistemas complexos; no entanto, sua implementação na Internet das Coisas (IoT) ainda enfrenta obstáculos em função das restrições dos dispositivos. O acesso deve ser descomplicado e ajustado para dispositivos com baixa capacidade, de modo a evitar sobrecarga no processamento e consumo excessivo de energia. Os estudos sustentam que um controle de acesso granulado é essencial para evitar que usuários ou dispositivos não autorizados realizem ações críticas na rede, como alteração de configurações industriais ou ativação de comandos remotos (Singh *et al*., 2023).

Finalmente, abordagens de defesa avançados, tais como a detecção de intrusões fundamentada no aprendizado de máquina, estão começando a ser incorporados ao ambiente da Internet das Coisas, a fim de complementar os protocolos de segurança convencionais. Modelos de detecção inteligentes revelam-se eficientes na identificação de padrões de anômalos de tráfego, comportamentos imprevistos de dispositivos e ataques distribuídos. Entretanto, pela razão do elevado custo computacional associado a essas abordagens, os cientistas sugerem que tais sistemas sejam implantados em *gateways* ou plataformas na nuvem, ao invés de serem colocados diretamente em dispositivos com recursos limitados. Forma, os modelos de inteligência artificial funcionam como uma camada extra de segurança, avaliando o comportamento dos dispositivos de Internet das Coisas em tempo real e gerando alertas ou ações de bloqueio preventivas ao identificar comportamentos suspeitos (Ramakrishnan *et al.*, 2020).

CONSIDERAÇÕES FINAIS

A Internet das Coisas (IoT) constitui um dos principais obstáculos da era digital, principalmente em razão da mistura de dispositivos exclusivos, restrições computacionais e do intenso trabalho de protocolos de comunicação leves. Neste estudo, obtém que a Internet das Coisas (IoT) se expande em uma escala global, integrando-se a contextos residenciais, empresariais, industriais e urbanos, além de que esse progresso proporciona vantagens substanciais para otimização e aprimoramento da eficiência operacional. Entretanto, a rápida

expansão revela vulnerabilidades específicas que exigem atenção, análise e mitigação constantes.

A avaliação dos capítulos evidenciou que os protocolos de comunicação — tais como MQTT, CoAP, AMQP e LoRaWAN — foram desenvolvidos com ênfase na eficiência e na redução de custos operacionais, o que foi concluído, por conseguinte, em lacunas significativas no que diz respeito à proteção de dados. Isso evidencia que a segurança em IoT deve ser considerada não como um elemento técnico adicional, mas como um componente fundamental na concepção, na arquitetura e na implementação dos sistemas.

Além das restrições técnicas, a Internet das Coisas (IoT) enfrenta desafios significativos em sua governança, como a inexistência de padronização entre os fabricantes, deficiências no ciclo de atualização de firmware, configurações impróprias e a carência de práticas de segurança que devem ser feitas tanto por usuários quanto por empresas. Esses elementos aumentam a superfície vulnerável e promovem ocorrências, como a invasão de dispositivos, a interceptação de informações, o sequestro de câmeras e aOs protocolos de segurança, como TLS, DTLS, IPsec e soluções fundamentadas em criptografia leve, revelam-se indispensáveis para atender a essas lacunas; No entanto, há dificuldades ao serem implementadas em dispositivos que possuem limitações de memória, energia e capacidade de processamento.

As restrições técnicas, a Internet das Coisas (IoT) enfrentam desafios significativos em sua governança, como a inexistência de padronização entre os fabricantes, deficiências no ciclo de atualização de *firmware*, configurações impróprias e a carência de práticas de segurança que devem ser impostas tanto por usuários quanto por empresas.

Assim, chega-se à conclusão de que a segurança na Internet das Coisas (IoT) é condicionada por um conjunto de fatores: protocolos protegidos , criptografia leve e eficaz, autenticação robusta, atualizações regulares, controle de acesso, monitoramento incessante e modelos de proteção planejados desde a fase de concepção — conhecido como "*security by design*".

Concluindo, a presente pesquisa oferece uma contribuição relevante para a compreensão técnica e conceitual dos protocolos de segurança em IoT, ressaltando a significância das investigações contínuas e da responsabilidade compartilhada entre fabricantes, desenvolvedores, administradores e usuários finais. um mundo cada vez mais interligado, investir em segurança se configurar não apenas como uma opção, mas como uma exigência

necessária para garantir a integridade, a privacidade e a confiança na revolução digital que a Internet das Coisas (IoT) representa.

REFERÊNCIAS

AL-QAHTANI, F. A Lightweight Security Protocol for IoT Communication. *Wireless Personal Communications*. Springer, 2020. Disponível em: https://link.springer.com/article/10.1007/s11277-020-07108-5. Acesso em: 20 nov. 2025.

ANAND, P.; KUMAR, R.; SINGH, A. Security Challenges in IoT Communication Using CoAP and MQTT. *Internet of Things Journal*. ScienceDirect, 2022. Disponível em: https://www.sciencedirect.com/science/article/pii/S2352864822000347. Acesso em: 20 nov. 2025.

CAVALCANTE, M.; OLIVEIRA, T.; SANTOS, J. Protocolos e Arquiteturas para IoT. *Intercursos – Revista Científica da UEMG*, 2022. Disponível em: https://revista.uemg.br/index.php/intercursosrevistacientifica/article/view/3712. Acesso em: 20 nov. 2025.

FERREIRA, A. R. Internet das Coisas e os Principais Protocolos. *Revista Intercursos*. UEMG, 2022. Disponível em: https://revista.uemg.br/index.php/intercursosrevistacientifica/article/view/3712. Acesso em: 20 nov. 2025.

KHAN, M.; PATHAN, A. IoT Security Risks and Protection Standards. *Springer Series in Security*, 2021. Disponível em: https://link.springer.com/chapter/10.1007/978-981-19-5936-3_12. Acesso em: 20 nov. 2025.

KUMAR, S.; RAO, V.; PATIL, K. Lightweight Cryptography for IoT Applications. *Journal of Network Security*. ScienceDirect, 2022. Disponível em: https://www.sciencedirect.com/science/article/pii/S2352864822000347. Acesso em: 20 nov. 2025.

MARTINS, R. Vulnerabilidades em Protocolos IoT. *Revista Intercursos*, 2021. Disponível em: https://revista.uemg.br/index.php/intercursosrevistacientifica/article/view/3712. Acesso em: 20 nov. 2025.

RAMAKRISHNAN, S.; DEEPA, R.; GOPAL, M. IoT Security Protocols and Attack Mitigation. *Wireless Personal Communications*, Springer, 2020. Disponível em: https://link.springer.com/article/10.1007/s11277-020-07108-5. Acesso em: 18 nov. 2025.

SINGH, R.; GUPTA, N.; KHAN, S. Secure and Energy-Efficient IoT Communication Protocols. *IEEE Internet of Things Transactions*, 2023. Disponível em: https://ieeexplore.ieee.org/document/10544115. Acesso em: 20 nov. 2025.

SOUSA, P.; LIMA, F.; ALMEIDA, V. Avaliação de Protocolos Seguros para IoT. *Google Scholar Indexed Papers*, 2021. Disponível em: https://scholar.google.com/scholar?hl=pt-BR&q=protocolos+de+segurança+para+iot. Acesso em: 19 nov. 2025.

WANG, X.; LIU, H.; ZHOU, P. Security Frameworks for IoT Messaging Protocols. *Wireless Communications*, Springer, 2020. Disponível em: https://link.springer.com/article/10.1007/s11277-020-07108-5. Acesso em: 18 nov. 2025.

ZHANG, Q.; HU, S.; CHEN, L. Advances in IoT Protocol Security. *Springer Lecture Notes in Networks and Systems*, 2021. Disponível em: https://link.springer.com/chapter/10.1007/978-981-19-5936-3_12. Acesso em: 18 nov. 2025.

IEEE. Secure IoT Communication Architecture. *IEEE Xplore Digital Library*, 2024. Disponível em: https://ieeexplore.ieee.org/document/10544115. Acesso em: 20 nov. 2025.

SPRINGER. Security Protocols for IoT Networks. *SpringerLink*, 2020. Disponível em: https://link.springer.com/article/10.1007/s11277-020-07108-5. Acesso em: 20 nov. 2025.

SCIENCEDIRECT. Security Challenges in IoT Applications. *Elsevier*, 2022. Disponível em: https://www.sciencedirect.com/science/article/pii/S2352864822000347. Acesso em: 20 nov. 2025.