

Uma visão preliminar de ferramentas *open-source* para IoT

Pedro Henrique Aquino Silva - 18102719

2020

Resumo

Este artigo consiste em uma revisão bibliográfica do tópico de Internet of Things (IoT). Especificamente, estima-se a quantidade e relevância de trabalhos relacionados ao desenvolvimento open source de soluções IoT, quais suas motivações, estado da arte, e alguns exemplos de trabalhos importantes publicados e apresentados em conferências ou revistas científicas dos últimos três anos são citados e comentados. Em particular, nota-se que a proposta da plataforma open source Atmosphere ([Berta et al., 2020](#)), particularmente interessante, devido às aplicações já em utilização e potencial de distribuição e uso por diferentes usuários a baixo custo. Também foi elaborada uma proposta de intervenção no projeto destas plataformas, com a ideia de incentivar a colaboração de código ou documentação e incluir testes psicométricos como forma de divulgação, assim como direcionamento do desenvolvimento para que elas atendam melhor as necessidades dos potenciais usuários e garantir que as plataformas sejam tão potentes ou viáveis quanto soluções proprietárias.

Palavras-chaves: Internet of Things, open source, IoT development, IoT performance

1 Introdução

1.1 Motivação

Soluções IoT devem se tornar cada vez mais comuns nos próximos anos. Enquanto grandes investimentos certamente serão realizados por empresas dedicadas à área e já estabelecidas, deve-se considerar que nem todos terão acesso à essas soluções, especialmente no caso de serem proprietárias e focadas no retorno de investimentos.

Para garantir que todos tenham acesso aos benefícios que poderão advir da expansão de IoT, e que os esforços do desenvolvimento não se concentrem nas estruturas de poucas empresas, trabalhos desenvolvidos pela comunidade e projetos de código aberto (*open source*) têm papel fundamental.

1.2 Justificativas

A Internet das Coisas é um tópico emergente nas pesquisas em redes de computadores, segurança e sistemas embarcados. É importante, para facilitar tais pesquisas, assim como o acesso do público aos benefícios dessa tecnologia, que soluções de código aberto recebam atenção e desenvolvimento.

1.3 Objetivos

1.3.1 Objetivos Gerais

Esse artigo visa avaliar qual o estado da arte em plataformas de Internet das Coisas *open source*. Assim, busca-se trazer visibilidade para os projetos de plataformas IoT, assim como promover ao autor um conhecimento maior das contribuições públicas da área.

1.3.2 Objetivos específicos

- Fomentar discussão acerca de tecnologias *open source* em IoT.
- Identificar o estado da arte em plataformas IoT de código aberto.
- Compreender quais projetos da área abrem possibilidade de contribuição para possíveis autores, pesquisadores e desenvolvedores, assim como potenciais usuários das plataformas utilizadas.

1.4 Organização do artigo

O presente trabalho está organizado em 8 seções posteriores à esta introdução.

Primeiramente, na seção “Conceitos básicos”, serão apresentados três conceitos fundamentais para a compreensão do trabalho, assim como dos artigos apresentados, notavelmente, os conceitos de *Internet of Things*, *open source* ou código aberto, e *IoT platforms*.

Em seguida, partiremos para a seção “Trabalhos correlatos”, na qual serão elencados 10 artigos relacionados ao tema. Destes, quatro artigos correlatos recentes, dos anos de 2020 e 2019, serão discutidos em maior detalhe, assim como sua relação com o tema do presente artigo. Os artigos selecionados são (Baba-Cheikh et al., 2020), (Berta et al., 2020), (Ghazanfar et al., 2020) e (Franco da Silva et al., 2020)

Segue a isto a seção “Aspectos relevantes”, discutindo de alguns tópicos comuns aos trabalhos selecionados. Incluem-se nesta seção discussões sobre disponibilidade e usabilidade dos *frameworks* abertos de desenvolvimento IoT existentes.

Faz-se então a identificação de desafios presentes, na seção “Problemas existentes”, como a própria dificuldade de desenvolvimento destas plataformas, aceitação na indústria

e na academia, problemas relacionados ao uso de plataformas proprietárias no ensino e pesquisa, entre outros.

Enfim, temos a seção “Soluções possíveis”, abordando a as possíveis intervenções propostas nos artigos avaliados em relação aos problemas identificados e mencionados na seção anterior.

Então, na seção “Proposta e desenvolvimento de uma proposta”, será apresentada uma proposta de solução relacionada a alguns dos problemas identificados nas etapas anteriores. Em particular, será analisada a proposta de um dos artigos apresentados, desta vez em sua completude.

Por fim, partimos para a seção “Conclusões e trabalhos futuros”, em que avaliaremos o trabalho realizado, assim como ressaltaremos os aspectos principais dos artigos analisados, assim como as propostas destes e trabalhos futuros no estado da arte de desenvolvimento IoT.

2 Conceitos básicos

2.1 IoT

Internet of Things (IoT) refere-se à interconexão digital de objetos à internet. A ideia é que se possa conectar desde aparelhos cotidianos até redes de sensores para proporcionar computações e facilidades novas aos usuários.

As aplicações de IoT variam desde comodidade em automação domiciliar até intensificação da eficiência produtiva do setor industrial e personalização do cuidado médico. As redes em aplicações IoT são formadas por “coisas” embarcadas de sensores, software e hardware que processem os dados coletados e os disponibilizem em ambiente “Fog” e “Cloud”, e acumuladas em servidores, onde são reprocessados a nível de aplicação disponíveis ao usuário. É uma das maiores tendências atualmente, em computação.

2.2 Open source

Open source é um termo usado com sentido de “código aberto”. Dizendo respeito a um *software* ou *hardware* que oferece livre acesso ao código fonte ou projeto, permitindo compartilhamento das ferramentas desenvolvidas entre os desenvolvedores, e quaisquer outras pessoas, sem restrição.

A ideia de projetos *open source* foi desenvolvida pela *Open Source Initiative* (OSI - não confundir com Open System Interconnection), com o objetivo de apresentar o software livre a empresas de maneira mais comercial, evitando questões éticas e de direitos de propriedade. Assim, não há também, custos de licenciamento, oferecendo a oportunidade de maior retorno de investimentos em serviços e formação.

Ao mesmo tempo, é importante diferenciarmos *open-source* de *software* livre ou *free software*. Enquanto a ideia de *open source* tem o propósito de estabelecer uma relação entre desenvolvedores e usuários em que o licenciamento seria simplificado, assim como oferecer verificação e maior confiabilidade ao cliente, que por sua vez saberia exatamente qual código estaria comprando; o *software* estabelece uma relação de “DIY”, por assim

dizer, em que o usuário final pode e é, de certa forma, incentivado a realizar alterações em sua cópia do produto, sem enfrentar implicações legais, exceto no caso de distribuição.

2.3 IoT platforms

Plataformas de Internet of Things (IoT platforms) são, em nível mais alto, o *software* que suporta a conexão entre *hardware* IoT, *access points* e redes de dados a outras partes da cadeia de valor, normalmente aplicações do usuário final. Normalmente lidam com o gerenciamento contínuo de tarefas e visualização de dados, o que permite que usuários gerenciem seu ambiente.

Podemos pensar nessas plataformas como o “encanamento” de um ambiente ou solução IoT; o meio entre os dados coletados no “Edge” e a aplicação final.

São, assim, uma camada crucial para o desenvolvimento de aplicações IoT, uma vez que boa parte dos protocolos de comunicação entre as “coisas” de uma rede e a própria camada de aplicação seria controlada ou ao menos facilitada por meio de uma plataforma IoT.

3 Trabalhos correlatos

Ao buscar em sistemas de agregação de artigos científicos pelas palavras chaves do tema, obtemos os resultados apresentados na tabela a seguir:

Palavras-chave	# Google Scholar
“IoT”	1.250.000
“IoT” “software”	397.000
“IoT platform”	292.000
“IoT” “open source”	216.000
“IoT” “open source” “platform”	143.000
“IoT platform” “open source”	11.100

Pela tabela, podemos ver que trabalhos que lidam com IoT e open source representam 17% do total de artigos relacionados a IoT. Em particular, o desenvolvimento de *IoT platforms* em ambientes *open source* representa pouco menos de 1% destes trabalhos. Enquanto existe um número significativo, iniciativas de código aberto para tecnologias de Internet das Coisas tem potencial de crescer ainda mais no meio científico.

Em particular, foram selecionados para análise 10 trabalhos recentes listados a seguir:

- *A Preliminary Study of Open-Source IoT Development Frameworks* ([Baba-Cheikh et al., 2020](#))
- *Atmosphere, an Open Source Measurement-Oriented Data Framework for IoT* ([Berta et al., 2020](#))
- *IoT-Flock: An Open-source Framework for IoT Traffic Generation* ([Ghazanfar et al., 2020](#))

- *MBP: Not just an IoT Platform* (Franco da Silva et al., 2020)
- *SAT-IoT: An Architectural Model for a High-Performance Fog/Edge/Cloud IoT Platform* (López Peña; Muñoz Fernández, 2019)
- *IoT Manager: a Case Study of the Design and Implementation of an Open Source IoT Platform* (Calderoni; Magnani; Maio, 2019)
- *The deployment of an IoT network infrastructure, as a localised regional service* (Fox; Donnellan; Doumen, 2019)
- *WoT-AD: A Descriptive Language for Group of Things in Massive IoT* (Le et al., 2019)
- *An Open Source Platform for Exploring NB-IoT System Performance* (Martiradonna et al., 2018)
- *Performance Evaluation of Open Source IoT Platforms* (Ismail; Hamza; Kotb, 2018)

Vamos agora comentar alguns aspectos de quatro destes trabalhos, nas seções seguintes.

3.1 A Preliminary Study of Open-Source IoT Development Frameworks

Neste trabalho, os autores estudaram uma amostra de quatro *frameworks* IoT de código aberto (no caso, Eclipse Vorto, ThingML, Node-RED e OpenHab), com *deploy* na plataforma Raspberry Pi, *hardware* tradicional no cenário de código aberto. Foi implementada uma seleção de três aplicações IoT, abrangendo diferentes domínios. Também comparou-se os quatro *frameworks* com um conjunto de critérios correspondentes ao mínimo de requisitos de aplicações IoT.

A problemática é identificar em que medida é que *frameworks* de código aberto suportam um conjunto mínimo de requisitos de aplicações IoT. Dado o conjunto de critérios apresentados neste artigo, nenhum dos *frameworks* estudados atingiu todos os critérios. Dentre os ambientes estudados, Node-RED e OpenHab são os que atingem o maior número de requisitos, oferecendo o melhor suporte para desenvolvimento IoT. Uma solução possível oferecida é a combinação destes dois *frameworks*. Existem algumas problemáticas acerca da validade do estudo, devido ao número limitado de aplicações implementadas, mas isso é abordado no artigo, com a ideia de aumentar a quantidade de aplicações e *frameworks* analisados, o que será feito como trabalhos futuros a curto prazo.

3.2 Atmosphere, an Open Source Measurement-Oriented Data Framework for IoT

Este trabalho consistiu no desenvolvimento de um *framework* orientado a medições para IoT. Os autores identificaram que, enquanto serviços de nuvem de IoT de última geração são poderosos, as melhores soluções são proprietárias, e há uma procura crescente de interoperabilidade e padronização. Os autores partiram para o estudo de como desenvolver

um sistema não específico a um vendedor, que explora o estado da arte de tecnologias de gerenciamento de dados, e visa o desempenho e desenvolvimento eficiente.

Concentração no conceito de medição, os autores abstrairam uma arquitetura que poderia ser aplicada numa variedade de domínios e contextos. Testaram o *framework* e o seu fluxo de trabalho em quatro casos de utilização, analisando dados e permitindo novos serviços em saúde, automóvel, e instrução. Os resultados do *framework* Atmosphere em diversas aplicações demonstraram a facilidade de uso e distribuição, além de flexibilidade do fluxo de desenvolvimento.

Nem todos os projetos em que o sistema foi utilizado foram finalizados, mas os que foram mostraram processos eficientes e promissores, permitindo a continuação da implementação em outros projetos. A contribuição original do projeto consiste em um modelo de computação *edge-to-cloud* usando recursos de rede IoT abstratos.

Por fim, o Atmosphere é um sistema projetado como um serviço de armazenamento de dados e suporte a computação, não vinculado a tecnologias *cloud* proprietárias e pronto para distribuição. Trabalhos futuros incluem enriquecer o conjunto de computações existentes, também utilizando processamento de aprendizado de máquina, assim como integrar medições psicométricas e dados de pesquisas de usuário, para suportar estudos de campo na aceitação dos usuários.

3.3 IoT Manager: a Case Study of the Design and Implementation of an Open Source IoT Platform

Novamente, neste estudo, os autores perceberam que a maior parte dos serviços e plataformas IoT são fornecidas por grandes empresas de tecnologia, no modelo de Software-as-a-Service (SaaS), evitando revelar o *know-how* envolvido no design e detalhes de implementação. Como consequência, universidades e instituições de ensino e pesquisa ficam impossibilitadas de explorar detalhes tecnológicos e estratégias de projeto que sustentem estas infraestruturas.

Como resposta a essa problemática, os autores propõem um *framework* projetado e implementado na Universidade de Bologna, Itália. O IoT Manager proposto foi desenvolvido como um sistema de gerenciamento de redes de sensores, cujo principal objetivo é fornecer à comunidade científica uma estratégia detalhada de implementação de plataformas e desenvolvimento IoT, de modo a disseminar tais tópicos de forma mais precisa e clara, tanto para pesquisa como ensino.

Os autores oferecem uma série de casos de uso para a plataforma proposta. Como trabalhos futuros, o texto sugere que o time focará em melhorar a camada de serviço, focando em interoperabilidade e expandindo a API da plataforma. Em primeiro lugar, afirma-se que um número maior de protocolos de comunicação devem ficar expostos para o *back-end gateway*, assim como o mapeamento *back-end* deveria ser oferecido juntamente com um conjunto maior de APIs de *engines* armazenamento externo.

3.4 WoT-AD: A Descriptive Language for Group of Things in Massive IoT

Este trabalho, diferentemente dos anteriores, consiste num exemplo de contribuição acadêmica para o campo de desenvolvimento IoT como um todo, para quaisquer plataformas, e serve como um exemplo de conhecimento compartilhando que o presente artigo deseja ressaltar.

Sendo assim, os autores identificaram que abordagens atuais de pesquisa tendem a prestar demasiada atenção à descrição de uma única Coisa. Assim, Os princípios de modelagem para linguagens de descrição de dispositivo IoT atuais são extremamente restritos em um cenário de Massive Internet of Things (MIoT) e Web of Things (WoT), por conta de requisitos de dissipação de custos operacionais e consumo energético.

Os autores propõem, então, uma linguagem de descrição de Assets com ojetivo de mitigar essas limitações, a *WoT based Asset Description*, ou WoT-AD. A WoT-AD explicitamente descreve um grupo de “Coisas” como um objeto homogêneo para permitir *mash-up*, *self-discovery* e simples acesso aos seus recursos, entidades e recursos. Os autores também propõem um *framework lightweight* que completamente integra WoT-AD de modo a permitir WoT para um cenário Massive IoT.

Segundo os autores, tal integração é eficiente na modelagem dos Assets, assim como simplifica o desenvolvimento de aplicações *mash-up* para usuários diferentes. A eficiência da solução projetada foi garantida pela escolha e combinação de tecnologias atuais e *frameworks* IoT que foram demonstrados na prática em casos de uso reais. Os trabalhos futuros consistem em avaliar e otimizar a WoT-AD em vários cenários IoT.

4 Aspectos relevantes

Nota-se pela leitura dos artigos correlatos alguns aspectos importantes que serão delineados a seguir.

O primeiro artigo delineou o fluxo de desenvolvimento de aplicações IoT utilizando alguns *frameworks* abertos disponíveis atualmente. Claramente, existe espaço para melhora tanto no que tange à aplicabilidade dos *frameworks* disponíveis como ao processo de desenvolvimento que eles carregam.

Contudo, os outros artigos mostraram que existem, ainda assim, plataformas IoT livres e abertas desenvolvidas no meio acadêmico que têm encontrado aplicações reais, assim como utilização no ensino voltado ao projeto, desenvolvimento e manutenção de tecnologias IoT. Sem estas plataformas, o ensino e pesquisa são dificultados pela indústria uma vez que o *software* utilizado não é disponibilizado em sua totalidade para estudo ou utilização por questões de propriedade intelectual.

Assim, os artigos mostraram que existem plataformas IoT de código aberto que fazem parte do conjunto de plataformas no estado da arte em gerência e desenvolvimento IoT. Estas plataformas estão em constante desenvolvimento e sua aplicabilidade tem bastante potencial de crescimento, ainda mais quando se leva em consideração o custo de utilizar uma solução proprietária.

O artigo ([Martiradonna et al., 2018](#)) apresentou também problemas relacionados a simulação e projeto de redes *Narrowband IoT*, ou NB-IoT, que surge como forma de

melhorar cobertura de rede e custos computacionais e de energia. Enquanto o desenvolvimento desta tecnologia tem grande contribuição da comunidade acadêmica e da indústria, existe necessidade de desenvolver ferramentas de modo a validar protocolos e testar e avaliar algoritmos para a NB-IoT stack.

Nota-se também, que plataformas IoT têm um papel central na arquitetura de software IoT e, segundo (Ismail; Hamza; Kotb, 2018), existem mais de 300 plataformas de desenvolvimento IoT registradas na literatura. Estas plataformas variam em capacidades e características. A complexidade do processo de seleção de uma plataforma IoT é aumentada quando se leva em consideração que as melhores soluções são proprietárias e isto pode afetar diretamente a alocação de recursos de um projeto IoT. Torna-se importante entender qual o estado da arte em plataformas de código aberto, gratuitas ou mais acessíveis, suas características básicas, e os requisitos a que atendem, de modo a permitir que a indústria se desenvolva sem custos exagerados de operação e desenvolvimento.

Um aspecto importante ressaltado em (López Peña; Muñoz Fernández, 2019) é que os novos e atuais padrões IoT não definem em suficiente detalhe aspectos importantes do suporte de computação Fog/Edge, do gerenciamento de computação IoT e dos sistemas de visualização IoT. Outros aspectos trazidos neste trabalho incluem a apresentação de conceitos de integração, automação e visualização de sistemas IoT, assim como um novo modelo arquitetural que permite atender outras demandas em IoT. A exemplo, a questão de oferecer serviços de segurança baseados em tecnologia *blockchain*.

Em resumo, o que demonstra grande demanda, dado que foi referenciado em todos os artigos, é padronização, interoperabilidade, acessibilidade, controle e acessibilidade no desenvolvimento IoT. Isto torna-se ainda mais explícito quando consideramos o contexto de *Massive Internet of Things* (Berta et al., 2020). Enquanto existem métodos de modelar e descrever facilmente “coisas” únicas por meio de linguagens diretamente instaladas em dispositivos, o movimento em direção a um cenário massivo de IoT leva ao surgimento de requisitos ainda mais intensivos em consumo de energia e custo de operação, trazendo novamente a noção de código aberto à frente.

5 Problemas existentes

Percebemos por meio dos artigos apresentados alguns problemas na implementação de serviços IoT que não utilizem soluções proprietárias.

A exemplo, segundo o primeiro artigo, os *frameworks* abertos disponíveis atualmente não encapsulam todos os requisitos do desenvolvimento IoT, deixando a desejar em escalabilidade ou performance. De fato, é relevante considerarmos que as soluções avaliadas por este artigo não são expressivas de todo o mercado de plataformas e *frameworks* abertos, o que é abordado pelos autores do artigo, com a sugestão de avaliar ainda outras plataformas e aplicações como trabalhos futuros. Ainda assim, é relevante para potenciais usuários notar que muitas das opções não-proprietárias disponíveis para o desenvolvimento de aplicações IoT podem não ter todos os requisitos cumpridos e este fato pode gerar atrasos e dificuldade no desenvolvimento destas aplicações.

Por outro lado, as plataformas apresentadas no segundo e terceiro artigos ainda estão em desenvolvimento, e a segunda, em particular, é puramente acadêmica. Enquanto,

a princípio, o desenvolvimento de uma solução voltada para educação não é um problema, a divulgação e adoção desta plataforma em cursos de *Internet of Things* ainda se mostra uma dificuldade.

Assim, os maiores problemas para a expansão de plataformas *open-source* em IoT consistem em limitações do desenvolvimento. Há, então, necessidade de ampliar o número de protocolos de comunicação suportados, melhorar questões de armazenamento, e possivelmente investir na utilização de otimizações proporcionadas por *machine learning* e outras tecnologias de ponta, como já é feito em soluções proprietárias.

Em resumo, o maior problema consiste em equiparar a performance e usabilidade destas plataformas a soluções proprietárias, e ampliar a aceitação de usuários para que elas possam ser utilizadas em mais aplicações reais, e enfim adequar-se aos requisitos do mercado. Enquanto passos tem sido tomados nesta direção, a capacidade do desenvolvimento colaborativo demonstrado em outras áreas com forte impacto *open-source* ainda não aparenta ter sido explorada em plataformas IoT.

Além disso, dos problemas de aceitação e distribuição de plataformas de código aberto, ainda existem problemas tecnológicos compartilhados pela indústria e academia, que abrem espaço para soluções *open-source*. A exemplo, há dificuldade de modelar e gerenciar sistemas de *Massive Internet of Things*, sendo que neste contexto, são requisitos básicos a escalabilidade, interoperabilidade e padronização, assim como baixo consumo de energia e custo de operação. Estes fatores são interentes ao crescimento massivo de redes de “coisas”, gerando a necessidade de desenvolvimento de ferramentas que auxiliem no projeto e gerenciamento de redes de tal magnitude.

Outro problema consiste na presente insuficiência da padronização e protocolos IoT focados tanto em computação Fog e Edge como na integração de sistemas NB-IoT e Cloud. Há ainda dificuldade de se selecionar IoT platforms que atendam todos os requisitos de um projeto sem grande elevação de custo de desenvolvimento e operação, papel no qual plataformas *open source*, como a Amosphere ([Baba-Cheikh et al., 2020](#)), se mostram particularmente atrativas.

Existe, ainda, uma dificuldade na prototipação e testes de redes IoT. Em ([Ghazanfar et al., 2020](#)), por exemplo, os autores afirmam a dificuldade de se analisar a segurança de rede em sistemas IoT, uma vez que a grande diversidade de redes IoT em termos de dispositivos, aplicações e protocolos que ferramentas geradoras de tráfego tradicionais são incapazes de produzir o tráfego específico de protocolos IoT. Este problema em específico será tratado na seção “Projeto e desenvolvimento de uma solução”.

6 Soluções possíveis

As soluções possíveis consistem no que foi exposto nos trabalhos comentados. A exemplo, a introdução de medições psicométricas e abertura a contribuições ao código podem não só melhorar o campo de aceitação do usuário, como também incorporar novas ideias ao código das plataformas existentes.

A introdução de medidas psicométricas nas plataformas existentes permite avaliar a resposta dos usuários às plataformas oferecidas atualmente, e realizar melhorias de acordo com estes dados, utilizando técnicas de análise de dados e aprendizado de máquina,

por exemplo.

Abrir o código a contribuições de desenvolvedores permite que novas soluções e otimizações sejam encontradas, utilizando-se do potencial colaborativo do *software livre*, assim como expandindo o campo de aplicação destas ferramentas IoT. Uma possibilidade de incentivo ao uso e contribuição das plataformas *open source* seria a participação em *hackathons* e outros eventos de desenvolvimento, além dos eventos acadêmicos e de divulgação científica já realizados.

Além disso, a utilização técnicas de aprendizado de máquina poderia auxiliar na otimização das plataformas atuais para equiparar seus desempenhos ao de soluções proprietárias disponíveis. Além disso, a abertura do código permite uma maior confiabilidade na coleta e processamento de dados, uma vez que o *software* que os analisa é aberto ao público, permitindo auditorias de privacidade — uma vez que isto também é uma preocupação do público geral no que tange utilização de soluções IoT em diversas áreas.

Quanto à ausência de plataformas de código aberto para ensino e uso acadêmico, foi-se proposto e demonstrado o uso de uma plataforma IoT desenvolvida com esse fim explícito, a IoT Manager (Calderoni; Magnani; Maio, 2019). Desenvolvida em ambiente acadêmico com o fim de facilitar pesquisas na área de gerenciamento de redes IoT, assim como o ensino das tendências do estado da arte de *software* em IoT platforms, esta plataforma vem como resposta à demanda de acesso ao código de ferramentas similares, que são em grande maioria proprietárias.

O problema descrito de modelagem e gerência de sistemas MIoT, foi-se proposto uma linguagem de descrição (WoT-AD) para grupos de “coisas” (Fox; Donnellan; Doumen, 2019), de modo que não haja necessidade explícita de descrever um único dispositivo na rede, permitindo maior integração da rede de objetos conectados em um contexto massivo. Além disso, foi proposto um *framework* de desenvolvimento que integra completamente a linguagem definida.

Como mencionado na seção anterior, existe dificuldade de se selecionar uma plataforma IoT dentre as opções disponíveis na literatura dadas as condições de custo e restrições de requisitos. Dentre as opções *open-source*, algumas foram selecionadas e detalhadas no artigo (Ismail; Hamza; Kotb, 2018).

No contexto de testes e geração de tráfego para protocolos IoT, por exemplo, foi desenvolvido um framework específico para IoT, o IoT-Flock, em contra-partida às ferramentas tradicionais de geração de tráfego. Novamente, este artigo em específico será comentado em detalhe na próxima seção.

7 Projeto e Desenvolvimento de uma Proposta

Nesta seção, iremos comentar a proposta desenvolvida no artigo *IoT-Flock: An Open-source Framework for IoT Traffic Generation* (Ghazanfar et al., 2020).

Este trabalho consiste em uma solução para o problema de gerar tráfego para validação e teste de protocolos IoT e de desempenho de soluções de segurança específicas para IoT. A problemática é que, devido à diversidade de redes IoT em termos de dispositivos, aplicações e protocolos, ferramentas tradicionais de geração de tráfego de rede

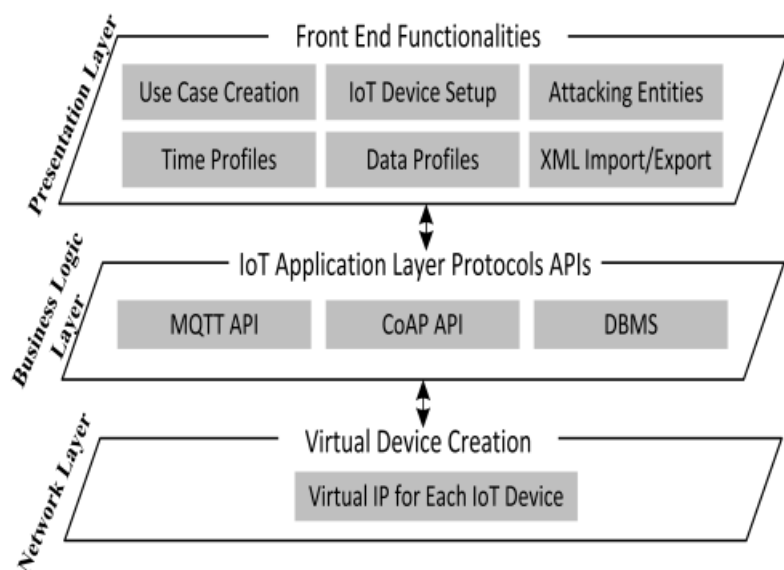


Figura 1 – Funcionalidades da IoT-Flock por camada

não conseguem produzir o tráfego necessário para avaliar redes IoT, dificultando projeto, validação e testes de algoritmos e protocolos voltados para IoT.

Desta forma, os autores desenvolveram um *framework* de código aberto baseado em IoT para geração de tráfego. Os desafios encontrados incluíram, principalmente, a modelagem de dispositivos IoT e a geração de tráfego IoT normal e de ataque simultaneamente. O *framework* denominado IoT Flock foi desenvolvido, sendo capaz de suportar dois protocolos IoT da camada de aplicação largamente utilizados, MQTT e CoAP. Este *framework* permite que um usuário crie um caso de uso, adicione dispositivos IoT customizados e gere tráfego normal e malicioso em tempo real em uma rede.

Como prova de conceito, demonstrando a aplicabilidade do *framework* proposto, foi-se criado um uso de caso de uma *smart home* IoT, permitindo o desenvolvimento de soluções de segurança para este ambiente a partir da emulação de dispositivos IoT reais. Os resultados, que serão discutidos a seguir, demonstraram que o *framework* apresentado efetivamente permite o desenvolvimento de soluções de segurança IoT melhores sem a necessidade de fisicamente implementar o caso de uso de tempo real.

A seguir, avaliamos em maior detalhe a estrutura proposta do IoT Flock. Primeiramente, uma visão das funcionalidades de cada camada do framework pode ser visto na figura 1.

Na camada de apresentação, pode-se definir o caso de uso a ser simulado, a rede IoT com a descrição dos dispositivos da rede IoT, entidades de ataque, duração de experimento, perfis de dados, além de se permitir importar e exportar todas as configurações de um experimento por meio de XML. Na camada *business logic*, tem-se as APIs que implementam os protocolos da camada de aplicação IoT, permitindo a realização das simulações determinadas pelo usuário. Por fim, a camada de rede consiste na geração de IPs virtuais para cada dispositivo IoT. Um diagrama mais detalhado do funcionamento da

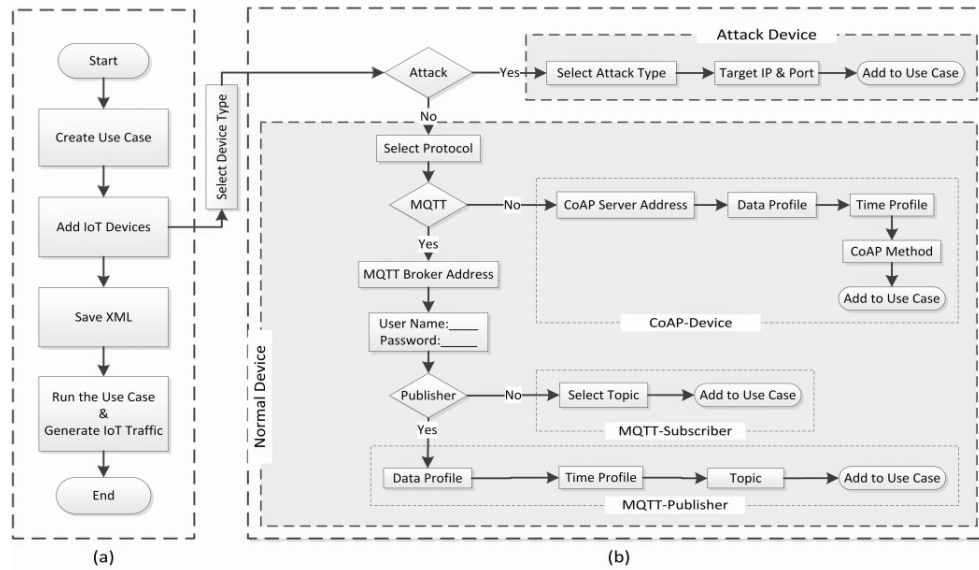


Figura 2 – Diagrama da IoT-Flock

TABLE II
ACTUAL TRAFFIC FEATURES

Device Name	Average Value	Mode	Average Time	Behavior
Temp Sensor	34.72 C	35 C	180s	Periodic
Light Sensor	120 Lux	100 Lux	180s	Periodic
Motion Sensor	0.5	1	3s-5s	Random
Humidity Sensor	40 %	42 %	180s	Periodic

TABLE III
EMULATED TRAFFIC FEATURES

Device Name	Data Profile	Time Profile	Behavior
Temp Sensor	33-35 C	180s	Periodic
Light Sensor	99-120 Lux	180s	Periodic
Motion Sensor	0-1	3s-5s	Random
Humidity Sensor	39-42 %	180s	Periodic

Figura 3 – Tabelas de dispositivos emulados no IoT-Flock, retiradas do artigo original

IoT-Flock é apresentado na figura 2.

Os ataques passíveis de serem emulados na IoT-Flock incluem *MQTT Packet Crafting Attack*, em que pacotes são criados especificamente para causar um *crash* em uma aplicação; *MQTT Publish Flood*, que causa um dispositivo envie mensagens em alta periodicidade, podendo causar um ataque *Denial of Service (DoS)*; *CoAP Segfault attack*, em que parte do pacote de *request and packet* é enviado como *null*, causando uma falha de segmentação — além disso, um ataque pode gerar um ataque DoS enviando tais pacotes em grande quantidade; e, por fim, *CoAP Memory Leak Attack*, no qual um ataque envia opções inválidas para o servidor CoAP, o que causa *memory crash*.

Para a validação do IoT-Flock como ferramenta de geração tráfego para redes IoT, foi considerado um cenário de *smart home*. A figura 3 refere-se aos dados reais e emulados pelo IoT-Flock. Foram treinados três algoritmos de *machine learning* de modo a desenvolver um sistema que identifique transferências de pacotes maliciosas, notavelmente, Naive Bayes (NB), Random Forest (RF) e K-Nearest Neighbor (KNN),

As métricas utilizadas na verificação foram sensibilidade, especificidade e precisão (*sensitivity, specificity, accuracy*) foram calculadas a partir das fórmulas apresentadas na figura 4.

$$Sensitivity = \frac{TP}{TP + FN} \times 100$$

$$Specificity = \frac{TN}{TN + FP} \times 100$$

$$Accuracy = \frac{TP + TN}{TP + FN + TN + FP} \times 100$$

Figura 4 – Fórmulas utilizadas na medição, extraídas do artigo original

TABLE IV
RESULTS

Parameters	NB	KNN	RF
Sensitivity	99.01	99.96	99.98
Specificity	95	0.99.88	99.99
Accuracy	97.14	99.92	99.99

Figura 5 – Tabela de resultados extraída do artigo original

Por fim, os resultados obtidos são apresentados na figura 5.

Podemos ver que IoT-Flock foi capaz de gerar tanto o tráfego de ataque como o normal, sendo uma solução para testar e treinar soluções de segurança em redes IoT. Três algoritmos de aprendizado foram utilizados e treinados para detectar tráfego malicioso para o caso de uso de uma *smart home*, sendo que o melhor foi encontrado no modelo de classificador Random Forest, com precisão de 99.99%.

8 Conclusões e trabalhos futuros

Neste trabalho, observou-se que o estado da arte em desenvolvimento de *IoT platforms open-source* está, atualmente, defasado em relação a soluções proprietárias, em especial no que diz respeito à usabilidade e escalabilidade.

Enquanto existem diversos frameworks que possibilitam o desenvolvimento de aplicações IoT que são abertos, gratuitos ou competitivos, existem poucos que cumprem todos os requisitos de uma aplicação real.

Além disso, existe dificuldade de se estudar o estado da arte de tais plataformas, uma vez que as mais comumente utilizadas e largamente disponíveis são proprietárias, o que normalmente acarreta em confidencialidade das técnicas desenvolvidas e empregadas na plataforma. Isto faz com que haja necessidade do desenvolvimento de plataformas acadêmicas, que podem apresentar técnicas não tão eficientes, uma vez que há alta probabilidade de projetos acadêmicos não obterem os mesmos níveis de financiamento que uma empresa especializada poderia direcionar a uma *IoT platform* proprietária. Além disso,

algumas plataformas proprietárias, como a própria IoT Manager (Ghazanfar et al., 2020).

Nota-se, também, pelos artigos (Franco da Silva et al., 2020) e demais, que existem grandes contribuições da comunidade acadêmica na área de *IoT platforms*, que costumam ser utilizadas na indústria. Isto reforça o vínculo existente entre a indústria e a comunidade de pesquisa, e demonstra a necessidade de transferência de tecnologia entre as áreas, de modo que a usabilidade e utilização das técnicas programáticas e *frameworks* utilizados no ensino e pesquisa sejam equiparados aos disponíveis em nível industrial.

Como forma de abordar estes problemas, identificou-se alguns problemas no atual desenvolvimento e distribuição das plataformas *open-source* existentes, elaborando-se uma proposta de intervenção com a abertura do código para desenvolvimento comunitário, como atualmente é feito com o *kernel* Linux, e a inserção de medidores psicométricos para permitir identificar adesão, aceitação e sugestões da comunidade de usuários, assim como verificar a usabilidade de plataformas como a Atmosphere (Berta et al., 2020) em uma diversidade maior de aplicações que o time de desenvolvimento principal consegue averiguar. Desta forma, espera-se identificar os pontos em que tais plataformas ainda se encontram atrás de plataformas proprietárias, assim como melhorar a distribuição, desenvolvimento e colaboração de desenvolvedores de plataformas IoT aos *frameworks* abertos disponíveis atualmente.

Dissertou-se também sobre o projeto do *framework* IoT-Flock, uma demonstração do espaço existente para software de código aberto dentro da pesquisa em redes IoT. Este *framework* oferece um gerador de tráfego dedicado a IoT, de modo que se possam validar ou treinar algoritmos de segurança em redes IoT, assim como simular cenários realistas de transferência de dados, sem a necessidade de se fazer a prototipação ou implantação física da rede.

Desta forma, notamos a importância da colaboração da indústria, academia e comunidade de desenvolvedores em plataformas e frameworks destinados para uso no projeto de sistemas de IoT e MIoT. Em particular, avaliamos alguns dos trabalhos recentes mais relevantes para redes IoT que levassem em conta ou propusessem ferramentas de código aberto, o que facilita o investimento e a comunicação entre a indústria, pesquisa, desenvolvimento e usuários finais de aplicações IoT.

Referências

Baba-Cheikh, Z. et al. A Preliminary Study of Open-Source IoT Development Frameworks. In: . New York, NY, USA: Association for Computing Machinery, 2020. (ICSEW'20), p. 679–686. ISBN 9781450379632. Citado 3 vezes nas páginas 2, 4 e 9.

Berta, R. et al. Atmosphere, an Open Source Measurement-Oriented Data Framework for IoT. *IEEE Transactions on Industrial Informatics*, p. 1–1, 2020. Citado 5 vezes nas páginas 1, 2, 4, 8 e 14.

Calderoni, L.; Magnani, A.; Maio, D. IoT Manager: a Case Study of the Design and Implementation of an Open Source IoT Platform. In: *2019 IEEE 5th World Forum on*

Internet of Things (WF-IoT). [S.l.: s.n.], 2019. p. 749–754. Citado 2 vezes nas páginas 5 e 10.

Fox, J.; Donnellan, A.; Doumen, L. The deployment of an IoT network infrastructure, as a localised regional service. In: *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*. [S.l.: s.n.], 2019. p. 319–324. Citado 2 vezes nas páginas 5 e 10.

Franco da Silva, A. C. et al. MBP: Not just an IoT Platform. In: *2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. [S.l.: s.n.], 2020. p. 1–3. Citado 3 vezes nas páginas 2, 5 e 14.

Ghazanfar, S. et al. IoT-flock: An open-source framework for IoT traffic generation. In: *2020 International Conference on Emerging Trends in Smart Technologies (ICETST)*. [S.l.: s.n.], 2020. p. 1–6. Citado 5 vezes nas páginas 2, 4, 9, 10 e 14.

Ismail, A. A.; Hamza, H. S.; Kotb, A. M. Performance Evaluation of Open Source IoT Platforms. In: *2018 IEEE Global Conference on Internet of Things (GCIoT)*. [S.l.: s.n.], 2018. p. 1–5. Citado 3 vezes nas páginas 5, 8 e 10.

Le, K. et al. IoT-AD: A Descriptive Language for Group of Things in Massive IoT. In: *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*. [S.l.: s.n.], 2019. p. 257–262. Citado na página 5.

López Peña, M. A.; Muñoz Fernández, I. SAT-IoT: An Architectural Model for a High-Performance Fog/Edge/Cloud IoT Platform. In: *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*. [S.l.: s.n.], 2019. p. 633–638. Citado 2 vezes nas páginas 5 e 8.

Martiradonna, S. et al. An Open Source Platform for Exploring NB-IoT System Performance. In: *European Wireless 2018; 24th European Wireless Conference*. [S.l.: s.n.], 2018. p. 1–6. Citado 2 vezes nas páginas 5 e 7.