|  |  |
| --- | --- |
| **MINISTÉRIO DA EDUCAÇÃO**  **INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE PERNAMBUCO**  **PRÓ-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO** | |

**RELATÓRIO PARCIAL DOS PROGRAMAS INSTITUCIONAIS DE INICIAÇÃO CIENTÍFICA**

## (2023 – 2024)

**Avaliação de desempenho e segurança do protocolo QUIC em dispositivos de Internet das Coisas.**

Relatório Parcial apresentado à Pró-Reitoria de Pesquisa, Pós-graduação e Inovação como parte dos requisitos do Programa de Iniciação Científica do IFPE, sob orientação do(a) Prof(a).

**Orientador: David Mota Junio Cavalcanti**

**Co-orientador: Ramon Mota de Souza Farias**

**DAVI SOUZA DE LUNA**

**CAMPUS IGARASSU**

**Março/2024**

**INTRODUÇÃO**

Este relatório parcial visa apresentar os resultados iniciais do projeto de pesquisa intitulado “Avaliação de Desempenho e Segurança do Protocolo QUIC em Dispositivos de Internet das Coisas”. O projeto aborda várias áreas, incluindo Internet das Coisas (ou IoT, do inglês *Internet of Things*) e suas aplicações, bem como os protocolos QUIC e MQTT.

A IoT é uma tecnologia que nos permite construir sistemas através da interconexão de dispositivos físicos na Internet, permitindo a troca de dados e o controle remoto desses dispositivos. No entanto, com o avanço da IoT, surge a necessidade por mecanismos de comunicação eficientes e seguros para lidar com o crescente volume de dados e garantir a integridade das informações transmitidas (MAGRANI,2018,p.24).

O protocolo MQTT desempenha um papel crucial na IoT, oferecendo um serviço de mensagens leve e eficiente, utilizando uma arquitetura *publish/subscribe* entre clientes e servidores. Ele é leve e projetado para ser facilmente implementado, sendo adequado para ambientes Machine-to-Machine e IoT, onde é necessário pouca demanda por recurso computacional, conservação de energia e largura de banda da rede é algo valioso[[1]](#footnote-0). O MQTT funciona por padrão sobre o TCP(Transmission Control Protocol), como observado em sua documentação¹. O TCP possui diversos desafios como o fenômeno de bloqueio do cabeçalho ou *Head-of-Line Blocking(SCHARF; KIESEL, 2006)*, que pode afetar a eficiência da comunicação. Há também o fato de que muitos protocolos *Wireless* também implementam *Automatic Repeat Request*(ARQ[[2]](#footnote-1)) na camada de enlace, o que pode prejudicar ainda mais o desempenho do TCP se o atraso da transmissão L2 for maior que o TCP RTO[[3]](#footnote-2)(SHANG,W.,2016). Além disso, a adição de criptografia TLS[[4]](#footnote-3) aos pacotes MQTT pode introduzir uma latência significativa de rede, quando combinada com os requisitos de tempo real e baixa latência frequentemente associados aos dispositivos IoT, pode representar um desafio adicional para a efetiva operação do sistema. Portanto, enquanto o uso do TLS é vital para garantir a segurança das comunicações, é essencial estar ciente dos possíveis impactos na performance e na eficiência do sistema MQTT em ambientes IoT.

Por outro lado, o protocolo QUIC é um protocolo da camada de transporte orientado à conexão que opera sobre o UDP. O QUIC representa uma alternativa ao protocolo TCP, por resolver problemas de *head-of-line blocking(SCHARF; KIESEL, 2006)* além de implementar a segurança de forma nativa através do TLS 1.3[[5]](#footnote-4), eliminando a necessidade de um estabelecimento de conexão adicional[[6]](#footnote-5). Diante do aumento do tráfego de dados na Internet e da crescente demanda por abordagens de segurança mais eficiente, incluindo em dispositivos IoT, faz-se necessário estudar alternativas que melhorem a eficiência e segurança no tráfego desses dados (MAGRANI,2018,p.24), e o QUIC como protocolo de estudo se mostra pertinente.

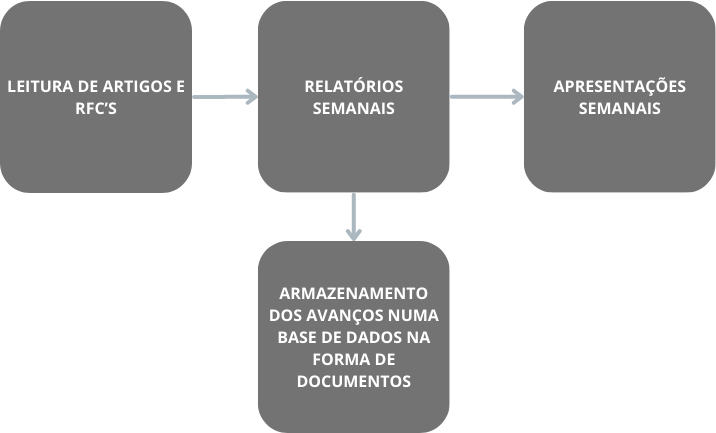
Dentro deste contexto, esta pesquisa vem se concentrando na análise de desempenho e segurança do protocolo QUIC em dispositivos IoT. A ideia é fazer as análises através de comunicações puramente QUIC, quanto utilizando o MQTT sobre o QUIC, aproveitando as vantagens de ambos os protocolos e uma vez que o MQTT está se tornado um padrão de facto para implementações de aplicações IoT (CAVALCANTI, D., CARVALHO, R. e ROSA, N. , 2021).

**METODOLOGIA**

Este estudo foi conduzido através de três etapas distintas, conforme descritas abaixo:

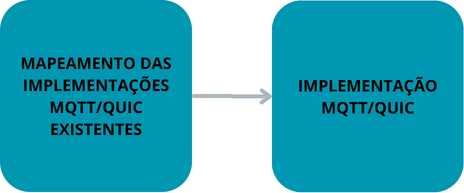
1. **Exploração Inicial:** No início do projeto foram realizadas sprints semanais, como delineado na Figura 1, que consistiram em:

* Leitura aprofundada de artigos e RFCs relacionados ao protocolo QUIC;
* Elaboração de relatórios visando preencher uma base de dados consolidada;
* Apresentações regulares para avaliar o progresso do conhecimento adquirido e para planejar as próximas etapas;



**FIGURA 1**

1. **Mapeamento de Implementações:** Após estabelecer uma base sólida de conhecimento sobre o protocolo QUIC, foram conduzidas sprints semanais dedicadas ao mapeamento de implementações existentes da pilha MQTT/QUIC, conforme ilustrado na figura 2.
2. **Implementação:** Mapeado as implementações, realizar sprints semanais para implementar a pilha MQTT/QUIC e relatar possíveis dificuldades durante essa etapa, como apresentado na figura 2;

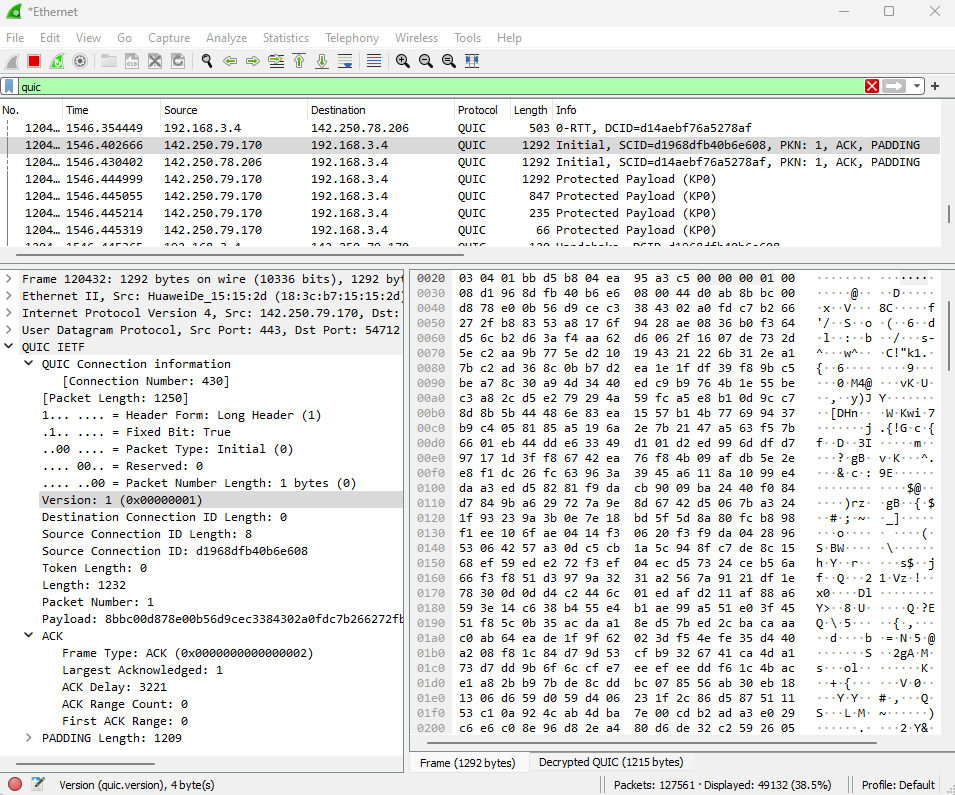
****

**FIGURA 2**

**RESULTADOS E DISCUSSÕES**

A primeira etapa do estudo foi concluída com sucesso, resultando na obtenção de uma base de conhecimento sólida sobre o protocolo QUIC. Esta conquista foi alcançada através de análises detalhadas dos pacotes QUIC, realizadas com o auxílio de um farejador de pacotes Wireshark[[7]](#footnote-6), conforme evidenciado na Figura 3. Também foi implementado[[8]](#footnote-7) funções simples de geração de cabeçalhos, gerador de ID de conexão e o frame PING e PADDING e a implementação de algoritmos de criptografia[[9]](#footnote-8) com o objetivo de aprendizado prático sobre como funciona o protocolo QUIC. Como ponto culminante desta etapa, foi realizada uma palestra durante a Semana Nacional de Ciência e Tecnologia no IFPE Igarassu. O principal objetivo dessa apresentação foi introduzir o protocolo QUIC aos estudantes do curso de Tecnologia em Sistemas para Internet, proporcionando-lhes uma compreensão abrangente e aprofundada deste importante protocolo de comunicação.

Na segunda fase, concentramo-nos no mapeamento de implementações já existentes da pilha MQTT/QUIC. Entre essas implementações, destacam-se os projetos desenvolvidos pela empresa EMQ Technologies[[10]](#footnote-9) e a NanoMQ Edge Computing[[11]](#footnote-10), incluindo EMQTT[[12]](#footnote-11), NanoSDK[[13]](#footnote-12) e NanoMQ[[14]](#footnote-13).

****

**FIGURA 3**

Atualmente o projeto de pesquisa encontra-se na terceira etapa com o objetivo de desenvolver e testar a pilha, enquanto é documentado quaisquer dificuldades encontradas ao longo do processo. Este relato detalhado de desafios enfrentados durante a implementação é crucial para a compreensão completa do contexto e de possíveis limitações de projeto.

**CONCLUSÃO**

Esta pesquisa foi criada com o objetivo de realizar uma análise abrangente do desempenho e segurança do protocolo QUIC em comparação com outros protocolos de transporte no contexto da Internet das Coisas(IoT). Ao longo das etapas concluídas até o momento, obtivemos uma base sólida de conhecimento sobre o protocolo QUIC, realizamos o mapeamento de implementações existentes da pilha MQTT/QUIC e estamos atualmente focados na implementação da pilha. Durante esse processo, documentamos cuidadosamente quaisquer desafios enfrentados, contribuindo para uma compreensão completa do contexto e possíveis limitações do projeto.

Considerando o progresso alcançado, é recomendado continuar com o acompanhamento rigoroso do desenvolvimento da pilha MQTT/QUIC, garantindo a resolução eficiente de quaisquer obstáculos encontrados. Esta pesquisa forneceu uma base sólida para investigações futuras e destaca a importância do protocolo QUIC no cenário emergente da IoT.

**PARECER DO ORIENTADOR**

1. **AVALIAÇÃO DAS ATIVIDADES DO(A) ESTUDANTE:**

O discente pesquisador Davi Souza de Luna executou adequadamente as atividades previstas no cronograma até a presente data. O objeto de pesquisa (protocolo QUIC e sua implementação em soluções IOT) do plano de trabalho é recente e consequentemente com documentações e casos de usos pouco difundidos. Como consequência do ineditismo da pesquisa o discente pesquisador enfrentou dificuldades, mas seu empenho e dedicação estão ajudando na resolução dos problemas. Para esta nova etapa da pesquisa (fase de implementação, testes e análises) a expectativa é que as atividades sejam realizadas com maior eficiência devido aos aprendizados anteriores. Portanto, o discente pesquisador encontra-se apto para a continuidade das atividades previstas no plano de trabalho.

**REFERÊNCIAS**

CAVALCANTI, D. J. M., CARVALHO, R. and ROSA, N. S., Adaptive Middleware of Things. 2021 IEEE Symposium on Computers and Communications (ISCC), Athens, Greece, 2021, pp. 1-6, doi: 10.1109/ISCC53001.2021.9631408.

SCHARF, M.; KIESEL, S. NXG03-5: Head-of-line Blocking in TCP and SCTP: Analysis and Measurements. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/4150963/>>.

SHANG, Wentao et al. Challenges in IoT networking via TCP/IP architecture. **NDN Project**, v. 2, 2016.

1. [https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.htm](https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html)l [↑](#footnote-ref-0)
2. <https://www.rfc-editor.org/rfc/rfc3366> [↑](#footnote-ref-1)
3. <https://www.rfc-editor.org/rfc/rfc6298> [↑](#footnote-ref-2)
4. <https://datatracker.ietf.org/doc/html/rfc5246> [↑](#footnote-ref-3)
5. <https://datatracker.ietf.org/doc/html/rfc8446> [↑](#footnote-ref-4)
6. <https://datatracker.ietf.org/doc/html/rfc9000> [↑](#footnote-ref-5)
7. <https://www.wireshark.org/> [↑](#footnote-ref-6)
8. <https://github.com/davisouzaluna/Dquic> [↑](#footnote-ref-7)
9. <https://datatracker.ietf.org/doc/html/rfc6234> [↑](#footnote-ref-8)
10. <https://www.emqx.com/en> [↑](#footnote-ref-9)
11. <https://github.com/nanomq> [↑](#footnote-ref-10)
12. <https://github.com/emqx/emqtt> [↑](#footnote-ref-11)
13. <https://github.com/emqx/NanoSDK> [↑](#footnote-ref-12)
14. <https://github.com/nanomq/nanomq> [↑](#footnote-ref-13)