CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
UNIDADE ARAXÁ

MARCO AURÉLIO RODRIGUES DE MAGALHÃES

IMPACTO NO PROCESSAMENTO E TEMPO DE TRANSMISSÃO EM REDE MODBUS TCP AO UTILIZAR TÉCNICA DE SEGURANÇA POR AUTENTICAÇÃO HB-MP*

ARAXÁ/MG
2024

MARCO AURÉLIO RODRIGUES DE MAGALHÃES

IMPACTO NO PROCESSAMENTO E TEMPO DE TRANSMISSÃO EM REDE MODBUS TCP AO UTILIZAR TÉCNICA DE SEGURANÇA POR AUTENTICAÇÃO HB-MP*

Trabalho de conclusão de curso apresentado ao Curso de Engenharia de Automação Industrial, do Centro Federal de Educação Tecnológica de Minas Gerais - CEFET/MG, como requisito parcial para obtenção do grau de Bacharel em Engenharia de Automação Industrial.

Orientador: Prof. Dr. Frederico Duarte Fagundes

ARAXÁ/MG

2024

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
COORDENAÇÃO DO CURSO DE ENGENHARIA DE AUTOMAÇÃO INDUSTRIAL / ARAXÁ

TRABALHO DE CONCLUSÃO DE CURSO – TCC – ATA DE DEFESA

ATA DE DEFESA DO TRABALHO DE CONCLUSÃO DE CURSO DE ENGENHARIA DE AUTOMAÇÃO INDUSTRIAL DO ALUNO **MARCO AURÉLIO RODRIGUES DE MAGALHÃES**

Às **quinze horas e trinta minutos** do dia **treze de setembro de dois mil e vinte e quatro**, reuniu-se, na sala 604 do Centro Federal de Educação Tecnológica de Minas Gerais - CEFET-MG/ Campus Araxá, a Comissão Examinadora de Trabalho de Conclusão de Curso para julgar, em exame final, o trabalho intitulado **IMPACTO NO PROCESSAMENTO E TEMPO DE TRANSMISSÃO EM REDE MODBUS TCP AO UTILIZAR TÉCNICA DE SEGURANÇA POR AUTENTICAÇÃO HB-MP***, como requisito parcial para a obtenção do grau de Bacharel em Engenharia de Automação Industrial. Abrindo a sessão, o Presidente da Comissão, Prof. **Frederico Duarte Fagundes**, após dar a conhecer aos presentes o teor das Normas Regulamentares do Trabalho Final, concedeu a palavra ao candidato, **Marco Aurélio Rodrigues de Magalhães**, para a exposição de seu trabalho. Após a apresentação, seguiu-se a arguição pelos examinadores, com a respectiva defesa do candidato. Ultimada a arguição, a Comissão se reuniu, sem a presença do candidato e do público, para julgamento e expedição do resultado final. Após a reunião da Comissão Examinadora, o candidato foi considerado: aprovado, obtendo nota final de: 89 /100 (oitenta e nove em cem). O resultado final foi comunicado publicamente ao candidato pelo Presidente da Comissão. O aluno, abaixo assinado, declara que o trabalho ora identificado é da sua autoria material e intelectual, excetuando-se eventuais elementos, tais como passagens de texto, citações, figuras e datas, desde que devidamente identificada a fonte original. Declara ainda, neste âmbito, não violar direitos de terceiros. Nada mais havendo a tratar, o Presidente encerrou os trabalhos. O prof. Frederico Duarte Fagundes, responsável pela disciplina "Trabalho de Conclusão de Curso II", lavrou a presente ATA, que, após lida e aprovada, será assinada por todos os membros participantes da Comissão Examinadora. Araxá, **treze de setembro de dois mil e vinte e quatro**.

Presidente e Orientador(a): Frederico Duarte Fagundes

Membro Titular: Sergio Luiz da Silva Pithon

Membro Titular: Leandro Resende Mattioli

Membro Suplente (caso tenha avaliado a defesa):

Professor da Disciplina TCCII: Frederico Duarte Fagundes

Aluno: Marco Aurélio Rodrigues de Magalhães

RESUMO

No contexto da automação industrial, a segurança, a velocidade e a eficiência na transmissão de dados são fundamentais. O protocolo Modbus TCP é amplamente utilizado em sistemas de automação industrial para comunicação entre dispositivos. No entanto, o desempenho e a segurança desses sistemas é uma preocupação crescente, especialmente no que diz respeito à integridade e confidencialidade dos dados. Este trabalho abordou a implementação da autenticação HB-MP* no protocolo Modbus TCP, analisando seu impacto no desempenho da rede em diferentes cenários. Inicialmente, foram realizados testes de desempenho, simulando a rede em uma única máquina, verificando os tempos com e sem a autenticação. Posteriormente, os testes foram estendidos para duas máquinas, implementando sobrecarga na rede por meio de transferência de arquivos e solicitações de Ping. Finalmente, mais dispositivos foram adicionados à rede, com quatro TV Boxes descaracterizadas simulando escravos para representar um cenário com maior densidade de dispositivos conectados. Os resultados revelaram um aumento significativo no tempo de transmissão com autenticação, indicando influência no desempenho da rede. Além disso, em cenário de sobrecarga por meio de transferência de arquivos, houve aumento no tempo de ciclo em comparação onde não houve sobrecarga na rede. Este trabalho contribui para o avanço do conhecimento em segurança em redes industriais, destacando a importância de equilibrar eficácia e desempenho na implementação de medidas de segurança.

Palavras-chave: Automação Industrial. Segurança em Redes. Protocolo Modbus TCP. Autenticação HB-MP*. Desempenho de Redes.

ABSTRACT

In the context of industrial automation, security, speed, and efficiency in data transmission are crucial. The Modbus TCP protocol is widely used in industrial automation systems for communication between devices. However, the performance and security of these systems are a growing concern, particularly regarding data integrity and confidentiality. This study addressed the implementation of HB-MP* authentication in the Modbus TCP protocol, analyzing its impact on network performance in various scenarios. Initially, performance tests were conducted by simulating the network on a single machine, verifying the transmission times with and without authentication. Subsequently, the tests were extended to two machines, implementing network overload through file transfers and Ping requests. Finally, more devices were added to the network, with four TV boxes simulating slaves to represent a scenario with a higher density of connected devices. The results revealed a significant increase in transmission time with authentication, indicating an impact on network performance. Additionally, in an overloaded scenario due to file transfers, there was an increase in the cycle time compared to when no network overload occurred. This study contributes to advancing knowledge in industrial network security, highlighting the importance of balancing effectiveness and performance in implementing security measures.

Keywords: Industrial Automation. Network Security. Modbus TCP Protocol. HB-MP* Authentication. Network Performance.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Nas últimas décadas, a automação industrial tornou-se uma força motriz em todos os sistemas de produção. Tecnologias e arquiteturas surgiram ao lado das crescentes estruturas organizacionais das plantas de produção. O avanço tecnológico e as demandas da indústria estabelecem que as empresas busquem soluções tecnológicas que visam (i) diminuir o atraso das respostas no processo, (ii) melhorar a qualidade dos produtos e (iii) aumentar a produtividade como forma de suprir as necessidades do mercado de consumo.

O monitoramento de processos e equipamentos de automação é uma pré-condição inerente para manter o processo de produção em condições quase ideais para cumprir os objetivos do negócio a curto, médio e longo prazo (BANGEMANN, 2014).

Através da implantação de protocolos de comunicação por onde ocorrem a troca de informações entre equipamentos, sensores, atuadores, máquinas, entre outros componentes, atualmente a utilização de redes industriais é um fator indispensável quando se quer obter informações e gerenciar processos (REYNDERS et al., 2005).

A integração das redes industriais com as redes de computadores tornou-se mais simples com o padrão Ethernet. Tem-se usado esse padrão para interconectar as operações industriais. O padrão Ethernet define o formato dos pacotes e protocolos para a camada de controle de acesso ao meio (MAC) (FAGUNDES, 2022).

Com o crescimento da utilização de tecnologias computacionais nas indústrias e corporações, aumentou-se a necessidade de garantir a confidencialidade, integridade e disponibilidade dos recursos dispostos em rede.

Quando se disponibiliza dados e equipamentos ao alcance de várias pessoas, cria-se um ponto de atenção: a segurança destes dados. Com a crescente utilização de componentes de redes e da internet, falhas podem ocorrer acidentalmente, devido a ruídos na comunicação e falhas de envio, ou, intencionalmente ocasionados por um atacante malicioso, invasões e infecções por vírus (VOLKOVA et al., 2019; GALLOWAY; HANCKE, 2013; CHEMINOD et al., 2018). Desta forma, surgiu então a necessidade primária de investimento na área de segurança de redes.

As técnicas de segurança de redes industriais são para prevenir essas falhas intencionais ou invasões causadas por agentes maliciosos, garantindo dessa forma a integridade na transmissão dos dados.

No contexto das redes industriais, o protocolo Modbus foi desenvolvido pela Modicon Industrial Automation Systems, hoje denominada de Schneider, e foi entregue no mercado em 1979, com o objetivo de comunicar um dispositivo, denotado como mestre com outros dispositivos, chamados de escravos. Não exigindo custos na aquisição de pacotes de software, tornou-se uma rede aberta que pode ser utilizada tanto em equipamentos industriais (sensores, atuadores, interfaces homem-máquina) quanto em aplicações fora do ambiente industrial, por meio de comunicação de leitura e escrita (MODBUS, 2016).

Normalmente utilizado sobre conexões seriais padrão como RS-232, RS-422 e RS-485, a Rede Modbus vem evoluindo e atualmente atende a conexão a partir de um padrão Ethernet. O padrão serial RS-485 continua sendo o meio físico mais utilizado atualmente para este protocolo (MODBUS, 2006).

O protocolo Modbus TCP/IP é um protocolo de mensagens sobre o meio físico Ethernet, sendo que TCP é um protocolo de nível de transporte, cuja função é realizar a comunicação entre aplicações diferentes e garantir a consistência para a integridade dos dados transmitidos. Ou seja, na comunicação entre dois nós TCP, cada equipamento deve ter um endereço IP (host) e especificar o número da porta TCP por onde será feita a comunicação de dados. Uma das vantagens da comunicação feita por Modbus TCP/IP é a facilidade de configuração de infraestrutura (MODBUS, 2012).

A rede Modbus TCP, por utilizar o padrão Ethernet para as camadas físicas e de enlace e por permitir a comunicação com diversos dispositivos e computadores, apresenta vulnerabilidade a ataques cibernéticos, pois esses ataques não requerem equipamento industrial específico e podem capturar, comprometer ou alterar os dados trafegados (FAGUNDES, 2022). Além disso, a rede Modbus TCP carece de ferramentas nativas de segurança.

Diante dessa limitação, em 2018 foi criado, pela organização Modbus, o novo protocolo de segurança denominado Modbus Security. O uso de protocolos seguros é um componente fundamental nos esforços para proteger o tráfego do Sistema de Controle. O protocolo oferece proteção por meio de *Transport Layer Security* (TLS) com o protocolo Modbus tradicional (MODBUS, 2018).

Uma desvantagem do Modbus Security é que, por utilizar algoritmo de criptografia, não tem compatibilidade para comunicação de dispositivos que ainda se comunicam com Modbus tradicional. Além disso, quanto maior a complexidade para a segurança na transmissão e dados, maior o tempo de transmissão, comunicação e processamento na rede.

Segundo FERST (2018), foi possível perceber ainda um aumento considerável no tempo necessário para estabelecer conexões usando o novo protocolo, o que pode inviabilizar o uso em ambientes críticos.

Sistemas de automação industrial priorizam processos com menor impacto no processamento e tempo de transmissão. Portanto, com a medição do tempo de transmissão e mais testes sob a tese de doutorado de segurança por autenticação HB-MP* elaborada por Fagundes (2022), com a implementação de novas funções, testes com sobrecarga na rede e possível implementação de algoritmo de criptografia, pode-se chegar a um resultado positivo e mais comprovações de que, mesmo com menor custo de processamento de memória e de comunicação, a técnica de segurança ainda seja vantajosa.

Diante estas considerações, através de uma técnica alternativa de segurança por autenticação HB-MP* estabelecida por (FAGUNDES, 2022), o presente trabalho teve por objetivo verificar e avaliar o impacto no processamento e tempo de transmissão em rede Modbus TCP ao utilizar técnica de segurança por autenticação HP-MP*. Além disso, foram implementados mais dispositivos conectados à rede para simular um cenário mais próximo da realidade industrial, onde é comum a comunicação entre múltiplos dispositivos. Esse aumento na densidade de dispositivos permite uma análise mais abrangente do desempenho do sistema, especialmente em condições de sobrecarga na rede, proporcionando uma avaliação mais precisa dos efeitos da autenticação em redes com alto maior tráfego de dados.

2 REFERENCIAL TEÓRICO

Alguns conceitos precisam ser resgatados para a discussão a respeito da segurança do protocolo Modbus, das técnicas utilizadas para sua segurança e do funcionamento do protocolo Modbus TCP. Este capítulo apresenta uma breve revisão sobre automação industrial, redes industriais e segurança em protocolo Modbus.

2.1 Automação Industrial

A automação industrial começou a ser objeto de destaque no mundo no século XVIII com o início da Revolução Industrial, originada na Inglaterra. Surgiu a necessidade de melhorar os processos de produção como forma de garantir maior rapidez e precisão em detrimento do trabalho manual, além de suprir as necessidades do mercado de consumo.

É comum pensar que a automação resulta do objetivo de reduzir custos de produção. No entanto, ela decorre mais de outras necessidades tais como maior nível de qualidade, expressa por especificações numéricas de tolerância, maior flexibilidade de modelos para o mercado, maior segurança pública e dos operários, menores perdas materiais e de energia, maior disponibilidade e qualidade da informação sobre o processo e melhor planejamento e controle da produção (BRANQUINHO, SEIDL, *et al.*, 2014).

Atualmente, automação industrial envolve a implantação de sistemas interligados e assistidos por redes de comunicação, em conjunto com sistemas de supervisão do tipo *Supervisory Control And Data Acquisition* (SCADA) e interfaces homem-máquina que auxiliam os operadores na supervisão e análise de processos produtivos e falhas que podem ocorrer (RIBEIRO, 1999).

A aplicação de automação nos processos industriais resultou em vários tipos de sistemas, que podem ser geralmente classificados como:

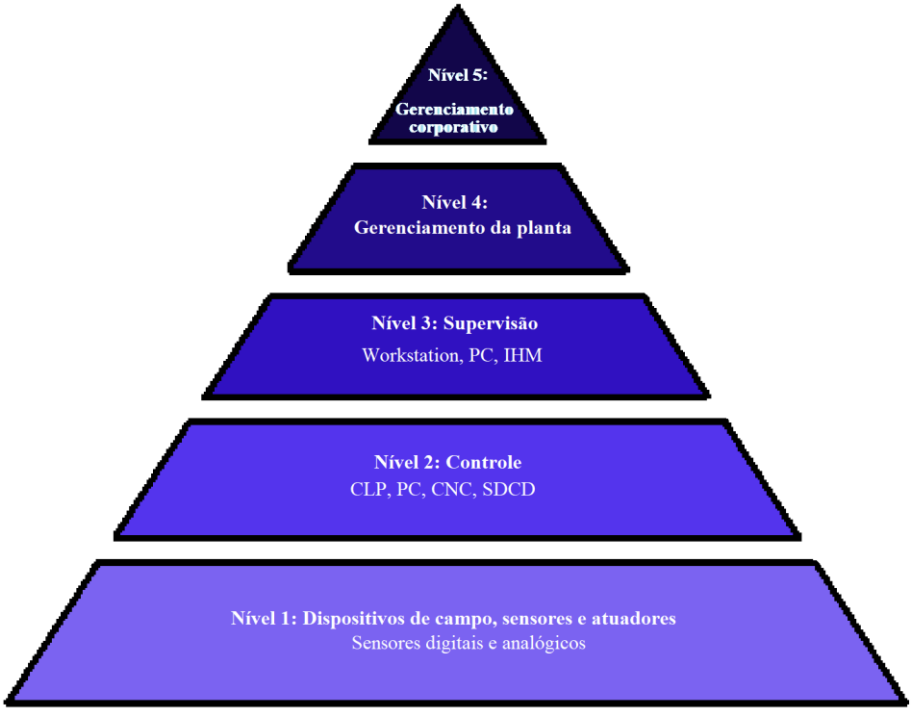
- Máquinas com controle numérico;
- Controlador lógico programável;
- Sistema automático de armazenagem e recuperação;
- Robótica;
- Sistemas flexíveis de manufatura.

2.1.1 Arquitetura da Automação Industrial

A arquitetura da automação industrial é constituída por diferentes níveis de automação (Figura 1), que tipicamente são:

- **Nível 1 -** também designado de “chão-de-fábrica”, é o nível das máquinas, dispositivos e componentes;
- **Nível 2 -** é composto por controladores digitais, dinâmicos e lógicos, associado a algum tipo de supervisão de processo. Neste nível encontram-se as Interfaces Homem-Máquina ou Interfaces (IHM) e as informações do nível 1;
- **Nível 3 -** onde acontece o controle do processo produtivo a partir da base de dados com informações da qualidade de produção, relatórios e estatísticas do processo;
- **Nível 4 -** é o nível responsável pela programação e planejamento de produção;
- **Nível 5 -** responsável pela administração dos recursos da empresa e de todo sistema, como pacotes de software para gestão de vendas e gestão financeira.

Figura 1 – Pirâmide de automação.



Fonte: Adaptado do Livro "Engenharia de Automação Industrial", 2014, 2ª Ed. Morais & Castrucci.

Através da implantação de protocolos de comunicação por onde ocorre a troca de informações entre equipamentos, sensores, atuadores, máquinas, entre outros componentes, a utilização de redes industriais é um fator indispensável quando se quer obter informações e gerenciar processos (REYNDERS, 2005).

2.2 Redes Industriais

As redes industriais, de acordo com Branquinho et al. (2014, p. 7), podem ser descritas como estruturas de comunicação bidirecional usadas para integrar equipamentos presentes em determinado subsistema responsável por parte do processo produtivo. Elas são protocolos de comunicação utilizados por sistemas supervisórios e de gerência, transmitindo e compartilhando dados entre si.

As redes industriais funcionam por meio de uma rápida troca de informações entre sensores, computadores, máquinas, atuadores, entre outros equipamentos. Elas surgiram no meio industrial com a finalidade de aperfeiçoar o controle dos instrumentos de campo, aumentar a capacidade de tráfego das informações e prover

mensagens de diagnósticos e configuração remota entre os componentes. (LUGLI e SANTOS, 2014)

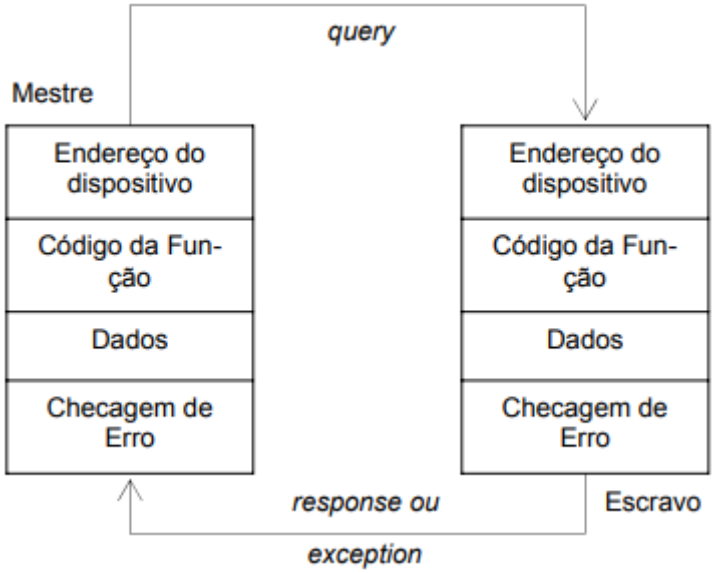
As redes se desenvolveram para incorporar todos os níveis em uma indústria através da adoção do padrão Ethernet, que facilita a integração das informações em campo, por ser utilizado nas redes de computadores nos níveis de gerenciamento e planejamento da empresa. Esse uso do padrão Ethernet foi motivado pela demanda de integração das informações em campo (FAGUNDES, 2022).

2.3 Protocolo Modbus

O protocolo Modbus é usado principalmente para estabelecer a comunicação entre dispositivos do tipo cliente e servidor onde um dispositivo tido como mestre, é responsável por iniciar as transmissões, e os outros, escravos respondem ao pedido do mestre (BRANQUINHO, SEIDL, *et al.*, 2014).

As mensagens desse protocolo podem ser do tipo *unicast*, quando o mestre envia uma requisição para um escravo específico e o mesmo responde, ou *broadcast*, quando o mestre envia uma requisição para todos os escravos e não é enviada nenhuma resposta conforme a Figura 2 (MODBUS, 2012).

Figura 2 – Modelo das mensagens Modbus.



Fonte: SENAI, 2014.

Esse protocolo é utilizado em grande escala por quase todos os fabricantes na comunicação entre autómatos programáveis, interfaces homem-máquina, sensores, atuadores, etc. Foi originalmente projetado para redes seriais assíncronas, como RS-232 e RS-485, com dois modos de transmissão, RTU e ASCII (SCHNEIDER AUTOMATION, 2006). Existe ainda o Modbus TCP, que utiliza o protocolo TCP/IP como camada de transporte.

2.3.1 Modbus TCP

Modbus TCP é um “protocolo de mensagens sobre o meio físico Ethernet, implementa o protocolo Modbus baseado em TCP/IP. Está contido na sétima camada do modelo OSI, a camada de aplicação. O protocolo de comunicação Modbus TCP opera através da configuração mestre/escravo” (MODBUS, 2012).

Uma das vantagens da comunicação feita por Modbus TCP é a facilidade de configuração de infraestrutura, através de switches ou hubs industriais, cabeamento de par trançado (com blindagem “STP” de preferência) e conectores RJ45 (MODBUS, 2012),

O Modbus TCP é utilizado em dispositivos de controle, como PLCs e em dispositivos de supervisão, como HMIs. Também pode suportar vários mestres e escravos, permitindo topologias de rede mais complexas e melhor escalabilidade em comparação com o Modbus RTU (MODBUS, 2012).

Uma desvantagem que a rede Modbus TCP apresenta é a falta de ferramentas nativas de segurança. Além disso, por utilizar o padrão Ethernet que permite a comunicação com diversos dispositivos e computadores, apresenta vulnerabilidade para ataques cibernéticos, pois esses ataques não requerem equipamento industrial específico e podem capturar, comprometer ou alterar os dados trafegados (FAGUNDES, 2022).

Para superar algumas dessas limitações, existem implementações e extensões do Modbus TCP que incluem recursos de segurança, verificações aprimoradas de integridade de dados e capacidades em tempo real. Essas implementações são frequentemente usadas em aplicações em que o protocolo básico do Modbus TCP não é adequado (MARSHALL, 2016).

2.4 Segurança em rede Modbus TCP

Quando se disponibiliza dados e equipamentos ao alcance de várias pessoas, cria-se um ponto de atenção, a segurança destes dados. Com a crescente utilização de componentes de redes e da internet, falhas podem ocorrer acidentalmente, devido a ruídos na comunicação e falhas de envio, ou intencionalmente, ocasionados por um atacante malicioso, invasões e infecções por vírus (VOLKOVA et al., 2019; GALLOWAY; HANCKE, 2013; CHEMINOD et al., 2018). Desta forma, surgiu então a necessidade primária de investimento na área de segurança de redes.

A integração das redes industriais com as redes de computadores tornou-se mais simples com o padrão Ethernet, que tem sido usado para interconectar as operações industriais. O padrão Ethernet define o formato dos pacotes e protocolos para a camada de controle de acesso ao meio (MAC) (FAGUNDES, 2022).

A rede Modbus TCP, por utilizar o padrão Ethernet para as camadas físicas e de enlace e por permitir a comunicação com diversos dispositivos e computadores, apresenta vulnerabilidade para ataques cibernéticos, pois esses ataques não requerem equipamento industrial específico e podem capturar, comprometer ou alterar os dados trafegados (FAGUNDES, 2022).

Segundo REYNDERS et al. (2005), as principais fontes de ameaças que afetam as redes de automação e as redes de computadores são:

- Grupos criminosos terroristas;
- Funcionários insatisfeitos;
- Serviços de inteligência;
- Espiões industriais.

As reais consequências dos ataques podem ser muito maiores do que simples falhas de software. Elas podem interromper a produção, danificando equipamentos, gerar graves acidentes e impactos ambientais. A proteção adequada de protocolos de redes industriais pode reduzir esses riscos (NEVES e SAUER, 2011).

De maneira a implementar esses protocolos em equipamentos de controle, os fabricantes

> apresentam as seguintes opções: ou modificam a implementação do protocolo de modo que ele não siga a especificação, sendo que o uso de criptografia impactaria no desempenho do processamento, gerando latência

> na rede, ou utilizam o protocolo mesmo sabendo que ele é vulnerável (BRANQUINHO, SEIDL, *et al*, 2014, p. 85).

Diante dessas informações, a proposta do trabalho é, através de uma técnica alternativa de segurança por autenticação HB-MP* estabelecida por Fagundes (2022), verificar a influência que a técnica tem no tempo de transmissão, comunicação, no processamento e no desempenho de uma rede Modbus TCP.

2.5 Vulnerabilidades em redes Industriais e em rede Modbus TCP

As redes industriais são suscetíveis a várias vulnerabilidades, que podem ser exploradas por atacantes cibernéticos para comprometer a segurança e operação de sistemas críticos. Com a profunda fusão da tecnologia da informação e da industrialização, cada vez mais sistemas de controle industrial tradicionalmente isolados estão diretamente conectados à internet, o que acelera a eficiência em compartilhamento de dados de produção, mas também introduz algumas ameaças à segurança (LANGNER, FALLIERE 2011).

Stuxnet é um dos casos mais notórios de ataque a uma rede industrial. Ele foi projetado para comprometer sistemas SCADA e PLCs em instalações nucleares. Stuxnet foi utilizado contra os equipamentos de enriquecimento de urânio do Irã entre os anos de 2009 e 2010. É considerado o primeiro ataque malicioso específico contra sistemas de controle industrial. Esse ataque atraiu ampla atenção tanto da academia quanto da indústria.

O ataque demonstrou a capacidade de malware altamente sofisticado de prejudicar sistemas de controle industrial críticos (CHEN; FALLIERE; MURCHU, 2011).

Em comparação com os protocolos de rede orientados a dados utilizados na internet, os protocolos de rede industrial, geralmente desenvolvidos a partir de versões seriais, são mais focados no controle de dispositivos físicos. Portanto, o uso de protocolos de rede industrial em infraestruturas críticas pode causar sérias consequências, como acidentes e poluição ambiental, colocando em risco a produção, os funcionários e a sociedade (CHEN, 2011).

As redes Modbus TCP apresentam diversas vulnerabilidades que podem ser exploradas por indivíduos maliciosos. Neste contexto, é crucial compreender as

vulnerabilidades de rede Modbus TCP e seus impactos, bem como examinar exemplos concretos de ataques que demonstram a realidade dessas ameaças.

Uma das vulnerabilidades mais comuns em redes Modbus TCP está relacionada à ausência de autenticação e criptografia adequada, embora tenha sido criado o protocolo de segurança Modbus Security em 2018, que oferece proteção por meio de Transport Layer Security (TLS) com o protocolo Modbus tradicional (MODBUS, 2018). A ausência de criptografia no protocolo Modbus tradicional facilita a interceptação de dados transmitidos, o que pode levar à exposição de informações confidenciais. Dessa forma, o invasor pode acessar e controlar dispositivos, como controladores lógicos programáveis (CLPs), de forma não autorizada (MODBUS ORG., 2012; HUITSING et al., 2008).

Um exemplo de ataque que ilustra essa vulnerabilidade é o chamado sniffing de rede, no qual um atacante utiliza ferramentas de monitoramento de tráfego de rede para capturar pacotes de dados Modbus TCP. Esses pacotes podem conter informações sensíveis, como configurações de dispositivos e até mesmo comandos de controle. A ausência de criptografia torna o processo de captura e interpretação desses pacotes relativamente simples, expondo as vulnerabilidades da rede Modbus TCP (ANUBHI; SANJAY, 2013).

Outra vulnerabilidade notável nas redes Modbus TCP é a falta de mecanismos de controle de acesso, como por exemplo a autenticação. Sem uma política de controle de acesso robusta, um dispositivo invasor na rede tem a capacidade de assumir o papel de Mestre e enviar requisições falsas aos outros dispositivos escravos. Isso abre a porta para ataques internos, causando interrupções na operação industrial ou mesmo danos físicos (ALOTAIBI et al., 2017; HUITSING et al., 2008).

Um exemplo de ataque de controle de acesso a essa vulnerabilidade é a técnica de spoofing de endereço IP. Nesse cenário, um atacante mascara seu endereço IP para se fazer passar por um dispositivo confiável na rede. Como a maioria das implementações Modbus TCP não verifica a autenticidade do dispositivo com base no endereço IP, um atacante pode capturar dados transmitidos na rede e obter informações relativas às identidades de usuários válidos, como endereços IP, e executar comandos maliciosos em nome de outro dispositivo, enviando informações falsas que podem causar danos significativos (GABRIELE et al., 2019).

Além disso, outros ataques que merecem atenção são os ataques de força bruta, homem-no-meio e ataques de Repetição (Replay Attack). Esses são outros

exemplos de ataques nos quais as redes industriais podem ser submetidas (FOVINO et al., 2009).

2.6 Estudos relacionados

Existem soluções propostas para abordar as vulnerabilidades nas redes Modbus, especialmente no protocolo Modbus-TCP, que é comumente usado em sistemas de automação industrial. Seja qual for a técnica implementada, fatores importantes devem ser considerados:

- Aumento da complexidade e tamanho do pacote de dados ao implementar determinada técnica de segurança;

- Longa vida útil dos equipamentos, garantindo que a técnica ainda seja eficiente com o equipamento operante;

- Impacto do tempo de transmissão e processamento com o aumento do pacote de dados transmitidos e a complexidade da técnica implementada.

Um estudo estabelecido por Osborn et al. (2020) discute e explora o uso de sistemas de detecção e prevenção de intrusões (IDPS – *Intrusion Detection and Prevention System*) com recursos de inspeção profunda de pacotes (DPI – *Deep Packet Inspection*) e firewalls industriais DPI, que têm a capacidade de detectar e interromper ataques altamente especializados ocultos no fluxo de comunicação. O estudo teve o objetivo de desenvolver assinaturas para o IDPS para ataques comuns a arquiteturas de rede baseadas em Modbus/TCP e avaliar o desempenho de três IDPS - Snort, Suricata e Bro - na detecção e prevenção de ataques comuns a sistemas de controle baseados em Modbus/TCP.

A DPI usada por firewalls industriais é uma forma de filtragem de pacotes que localiza, identifica, classifica, redireciona ou bloqueia pacotes com dados específicos ou cargas úteis de código que a filtragem de pacotes convencional, que examina apenas os cabeçalhos dos pacotes, não consegue detectar (J. NIVETHAN; M. PAPA, 2016). O IDPS com recursos de DPI é capaz de usar assinaturas para detectar e reduzir a probabilidade de um ataque bem-sucedido ao escravo Modbus/TCP. Semelhante ao IDPS, um firewall industrial pode ser usado como uma ferramenta de DPI.

Os resultados apresentados no artigo ilustram que pode ser uma tarefa desafiadora atingir os requisitos de comunicação em tempo real em alguns sistemas de controle industrial e de automação, caso a DPI seja implementada, devido à latência e ao *jitter* (variação no atraso de pacotes de dados durante a transmissão) introduzidos por esses IDPS e firewall industrial de DPI (Osborn et al., 2020).

Um outro estudo estabelecido por Fovino et al. (2009) investigou o impacto de malwares, como Code Red, Nimda, Slammer e Scalper, em sistemas SCADA usando o protocolo Modbus. Eles desenvolveram dois malwares específicos para atacar dispositivos Modbus TCP: um para ataques DoS e outro como um worm para explorar e prejudicar sistemas SCADA.

Fovino et al. (2009a) propuseram uma solução para melhorar a segurança do protocolo Modbus. A solução inclui a adição de mecanismos de segurança, como uma estampa de tempo e um valor hash encriptado ao quadro. Essa implementação busca equilibrar a segurança sem comprometer significativamente o desempenho de sistemas em tempo real. A solução utiliza uma assinatura digital para integridade e autenticidade, juntamente com uma estampa de tempo para evitar ataques de repetição de pacotes. A estampa de tempo é proveniente de um servidor NTP na mesma rede do sistema SCADA. Resultados experimentais mostraram um aumento negligenciável no tamanho do pacote de dados e na latência do protocolo, com um overhead de 32 bytes por quadro, sendo mais significativo para funções de baixa transmissão de dados e menos impactante para funções que envolvem mais dados.

2.7 Autenticação HB-MP*

A autenticação HP-MP* é uma técnica que pertence à família de protocolos HB (Hopper-Blum) e é projetada para oferecer segurança em redes de comunicação com recursos limitados. É particularmente útil em cenários de segurança de redes industriais, onde a complexidade das técnicas de segurança pode ser um fator crítico devido às restrições de processamento e memória (ASEERI et al., 2016).

Segundo Hopper (2001), a principal ideia por trás da autenticação HP-MP* é sua utilização em dispositivos microprocessados e de RFID. Essa aplicação, segundo Fagundes (2022), pode ser utilizada em operações simples, com baixo uso de recursos computacionais e de comunicação, apresentando eficácia na proteção de

redes industriais contra ameaças, como acesso não autorizado, gravações não autorizadas e injeção de respostas por dispositivos invasores.

Conforme Aseeri et al. (2016), aqui estão alguns aspectos-chave da autenticação HP-MP*:

Chave Compartilhada: A autenticação HP-MP* envolve o uso de uma chave compartilhada entre os dispositivos envolvidos na comunicação. A chave deve ser um número primo e deve ser representada por um número primo de bits.

Operações Simples: O protocolo HP-MP* utiliza operações simples no nível binário, o que minimiza o processamento e a carga de comunicação. Essas operações incluem operações bit a bit, como OU Exclusivo (XOR) e rotação de bits.

Geração de Desafios e Respostas: Um dispositivo autenticador gera um desafio aleatório e o envia para o dispositivo a ser autenticado. O dispositivo a ser autenticado responde com uma operação que inclui o desafio, a chave compartilhada e um valor de ruído. O dispositivo autenticador realiza a mesma operação e verifica se a resposta coincide com a resposta calculada.

Inclusão de Ruído: O ruído é introduzido intencionalmente nas respostas para dificultar a descoberta da chave secreta por um invasor que possa ter acesso aos dados trafegados.

Autenticação Após Múltiplos Ciclos: Devido à presença de respostas incorretas devido ao ruído, a autenticação não é baseada em um único ciclo, mas após uma quantidade específica de ciclos bem-sucedidos, garantindo maior segurança.

A autenticação HP-MP* para aplicações em redes industriais, onde a segurança é essencial e os recursos de processamento e comunicação são limitados, fornece uma camada adicional de segurança, mesmo em redes onde outras técnicas de segurança podem ser implementadas em outras camadas (FAGUNDES, 2022).

3 METODOLOGIA

Inicialmente, foi realizada a análise bibliográfica para uma melhor compreensão do tema, com a finalidade de elencar problemas de segurança na transmissão de dados do protocolo Modbus TCP e as soluções já existentes. Os temas pesquisados foram: Segurança em rede Modbus TCP; Autenticação HB-MP*; e Eficiência na transmissão de dados.

Para a pesquisa, foram utilizadas as bases de dados IEEE, SCOPUS e Google Scholar, entre outras, com os termos chave Modbus, redes industriais, segurança em redes industriais e transmissão de dados. Para os estudos relacionados, foram selecionados apenas aqueles com data de publicação a partir de 2016.

Após a pesquisa e estudo, para validação da proposta, as principais ferramentas de hardware e software utilizadas estão descritas abaixo:

- PC 1: um computador pessoal (laptop) com sistema operacional Windows 11, processador Intel Core i5 e 16GB de memória RAM. O PC 1 será o hospedeiro (host) do Mestre HB Modbus e do Escravo HB Modbus;
- PC 2: um computador pessoal (laptop) com sistema operacional Windows 10, processador Intel Core i5, 8GB de memória RAM. O PC 2 é o hospedeiro do simulador de Escravos ModbusPal e do Escravo HB Modbus;
- Switch Intelbras com oito portas fast Ethernet SF 800 Q;
- Aparelhos TV Box descaracterizados, com sistema operacional GNU/Linux, memória RAM 1 GB e 16 GB de armazenamento, utilizadas para atuar como componentes escravos na rede Modbus TCP/IP;
- Cabo Ethernet categoria 5e: utilizado para conectar os PC 1, PC 2, estabelecendo-se a rede com conexão direta e também o PC 1 com as quatro TV boxes, estabelecendo-se a rede através do switch;
- ModbusPal: software simulador de Escravos Modbus desenvolvido em linguagem Java, para verificação da compatibilidade das requisições HB Modbus com escravos Modbus tradicionais. Foi instalado no PC 2;

- Plataforma IDLE: ambiente de desenvolvimento integrado (IDE – Integrated Development Environment) para programação em linguagem Python. É uma plataforma de linguagem Python, fornecida diretamente no site oficial python.org. Foi instalada no PC 1 e no PC 2.

Os recursos de hardware, que são os PCs 1 e 2, as TV boxes e os cabos Ethernet, são mostrados na Figura 3 e Figura 4. A visão geral da infraestrutura da rede é mostrada na Figura 5.

Figura 3 – Hardwares utilizados para realização dos testes: PC 1, PC 2 e cabos Ethernet

Fonte: Elaborada pelo autor

Figura 4 – Hardwares utilizados para realização dos testes: quatro TV Box, Switch e cabos Ethernet

Fonte: Elaborada pelo autor

Figura 5 – Infraestrutura da rede contento as 4 TV box, PC, switch e cabos Ethernet

Fonte: Elaborada pelo autor

O trabalho foi feito com base no código fonte inicial de Fagundes (2022). Foram feitas modificações no código fonte inicial da técnica de segurança por autenticação HB-MP* para medições de tempo RTT (*Round Trip Time*) e tempo de ciclo. Não foram implementadas novas funções Modbus para os mestres e escravos.

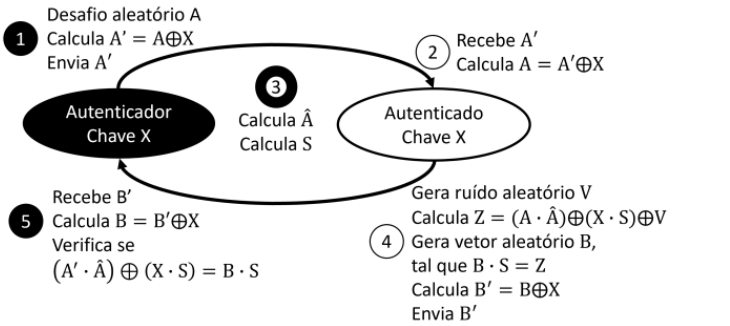
A ausência de implementação de novas funções decorre do fato de que funções diferentes de leitura e escrita não apresentam diferenças significativas nos tempos de transmissão e processamento na rede. Isso é especialmente relevante considerando que a aplicação inicial de Fagundes (2022) consistia apenas na utilização da função de escrita em um registrador.

3.1 Programação da Autenticação HB-MP*

Na parte de programação do protocolo HB-MP* o desenvolvimento seguiu exatamente a proposta estabelecida por Fagundes (2022), com todos os parâmetros, ajustes e testes já estabelecidos para garantir melhor eficiência da técnica e evitar falsos positivos e falsos negativos, para que um dispositivo não autêntico não seja identificado como autêntico. O protocolo HB-MP* foi desenvolvido com o propósito de efetuar a autenticação, seguindo os procedimentos detalhados no capítulo anterior e resumidos no diagrama de Máquina de Estados apresentado na Figura 6. No

processo, o nó autenticador realiza os passos 1 e 5, enquanto o nó autenticado executa os passos 2 e 4, e ambos os nós participam da execução do passo 3.

Figura 6 - Processo de autenticação com protocolo HB-MP*.



Fonte: Fagundes (2022).

O processo de autenticação foi incluído como parte do protocolo da camada de aplicacação Modbus. Com isso, após a conexão TCP, um Mestre envia uma requisição Modbus e um desafio modificado (A') ao Escravo conectado. O Escravo deve executar a requisição e enviar de volta uma resposta Modbus, bem como a resposta modificada (B') ao desafio HB-MP*. Com (B') o Mestre é capaz de verificar a autenticidade do Escravo (FAGUNDES, 2022).

3.2 Testes do impacto da autenticação na comunicação

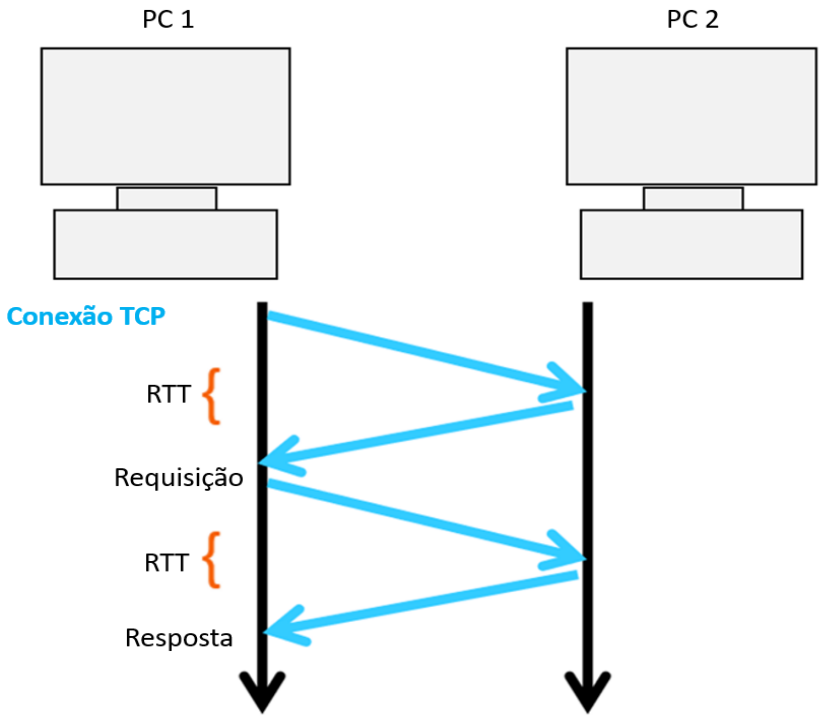
A validação da proposta do HB Modbus já foi realizada anteriormente por Fagundes (2022), bem como alguns testes de funcionalidade e testes de proteção com a implementação da autenticação. Desta forma, foram abrangidos neste Trabalho de Conclusão de Curso os testes de desempenho na rede.

Para avaliar o impacto da camada de autenticação no desempenho da rede, foram realizadas medições de RTT e tempo de ciclo. No âmbito das redes industriais, o RTT é um parâmetro de extrema importância, representando o intervalo temporal entre o envio de um pacote de dados de um ponto de origem para um destino e a recepção da resposta correspondente. Essa medida é fundamental para avaliar o

desempenho e a eficiência da comunicação em ambientes onde a precisão temporal e a confiabilidade são cruciais.

Ao considerar a aplicação prática da medição do RTT em uma rede Modbus entre dois computadores , é essencial compreender as nuances dessa configuração, onde a comunicação ocorre sobre a pilha de protocolos TCP/IP. Essa escolha proporciona um cenário mais representativo dos ambientes industriais contemporâneos. A Figura 7 abaixo ilustra a medida RTT.

Figura 7 – Esquema de medida do tempo RTT entre duas máquinas



Fonte: Adaptado de StormIT

O cálculo do RTT envolve o envio de um pacote (por exemplo, um pacote ICMP Echo Request em caso de ping) de um dispositivo para outro e a medição do tempo decorrido até que o pacote de resposta correspondente seja recebido. O Código abaixo apresenta a implementação em Python para calcular tempo RTT.

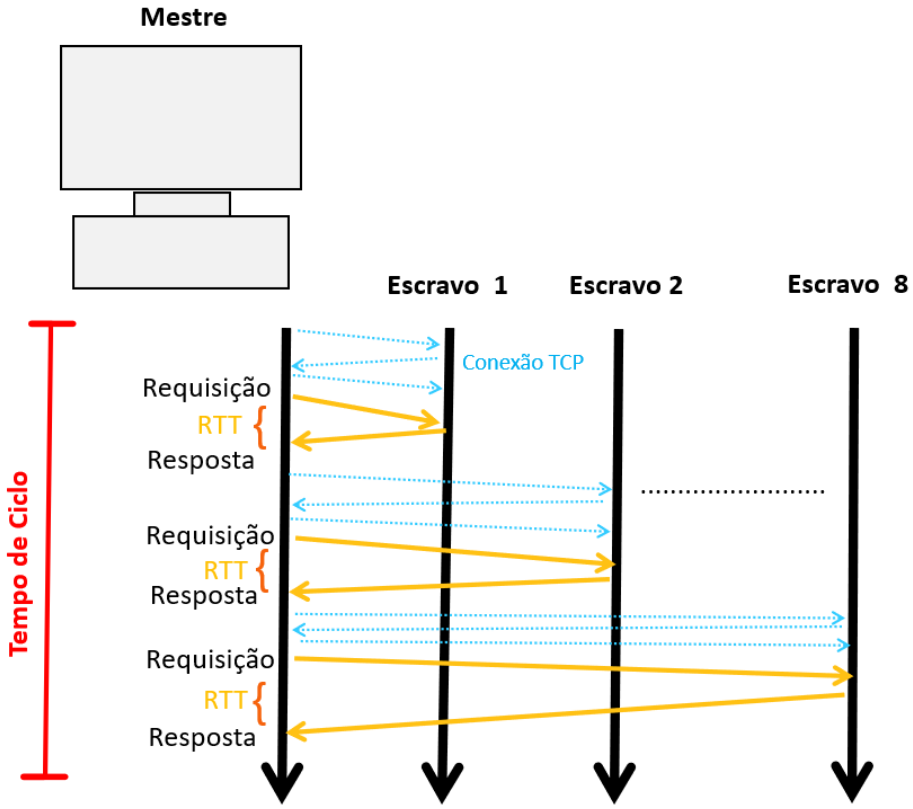
```
def measure_rtt(sock, req):
    start_time = time.time()  # Registra o tempo de início
    sock.send(req)  # Envio da solicitação
    rec = sock.recv(BUFFER_SIZE)  # Recebimento da resposta
```

```
        end_time = time.time()  # Registra o tempo de término
        rtt = end_time - start_time  # Calcula o RTT
        return rtt
```

A unidade de medida do RTT geralmente é em milissegundos (ms) e seu valor pode variar dependendo de vários fatores, incluindo a distância física entre os dispositivos, a qualidade da infraestrutura de rede, a carga da rede e outros elementos que podem introduzir atrasos na transmissão de dados. A análise do RTT é uma prática comum em diagnósticos de rede e monitoramento para garantir um desempenho adequado.

Além do tempo RTT foi medido o “tempo de ciclo” da rede Modbus com oito escravos, esse tempo refere-se ao intervalo de tempo necessário para concluir uma iteração completa de comunicação, que envolve a leitura e/ou escrita de dados entre o mestre e cada um dos oito escravos. A complexidade da rede aumenta com o número de escravos, e o tempo de ciclo é influenciado pela quantidade de dados a serem transmitidos, a taxa de atualização dos dispositivos e a eficiência do protocolo Modbus. A Figura 8 ilustra o tempo de ciclo para rede Modbus TCP contendo 8 escravos.

Figura 8 – Representação de conexão TCP, tempo de ciclo e tempo RTT



Fonte: Adaptado de Fagundes (2022).

O primeiro teste visou comparar o RTT com e sem autenticação HB-MP*. Para isso, foi feita a análise do RTT com Mestre HB Modbus e Escravo HB Modbus sendo executados na mesma máquina. O RTT foi medido cem vezes com a autenticação HB-MP*. Para comparação, os programas foram modificados para não executar a autenticação HB-MP*. Com isso, o RTT foi medido novamente por cem vezes, e os valores foram comparados.

A execução repetida dos testes em máquinas separadas proporcionou uma compreensão mais abrangente do impacto da autenticação na comunicação entre dispositivos, reproduzindo as condições típicas de uma rede industrial.

Similar ao primeiro teste, o RTT foi medido entre as duas máquinas, foram realizadas um número de cem medições com a programação da autenticação e, posteriormente, cem medições sem o código de autenticação.

Além da medição do RTT, também buscando medir o impacto da autenticação, o tempo total de ciclo foi medido, com oito escravos sendo simulados no PC 2. De forma similar, foram realizadas cem medições do ciclo das iterações completas entre

o mestre e os oito escravos com a implementação da autenticação e cem medições sem o programa de autenticação.

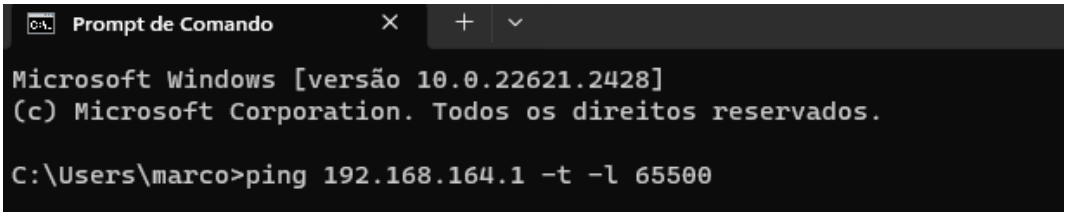
Outro fator importante mensurado e observado foi a variância dos tempos de transmissão, sendo que em contextos como redes industriais, um alto valor de variância nos tempos de transmissão pode indicar uma maior probabilidade de ocorrência de *jitter* na transmissão de dados. Se os tempos de transmissão variam significativamente em relação à média, isso pode resultar em pacotes chegando mais cedo ou mais tarde do que o esperado, causando *jitter* na transmissão (LI, 2008). Os resultados das medições estão descritos na seção 4.

3.3 Medição de RTT e tempo de ciclo com sobrecarga na rede

Além do impacto da autenticação na comunicação Modbus, a técnica de autenticação também foi testada em cenários de sobrecarga na rede. Em um dos cenários, foi efetuada a simulação de "*Ping flood*", com ping bidirecional na rede estabelecida entre o PC 1 e o PC 2 com conexão direta e física por meio de um cabo Ethernet. Para esse teste, foram desabilitados temporariamente os firewalls e os sistemas de proteção que pudessem interferir nos procedimentos, garantindo assim que os resultados refletissem o impacto direto do *Ping flood* na rede, sem restrições externas.

O teste foi realizado com o comando ping, disponível na interface do Prompt de comando do Windows. Configurar o comando ping para induzir um *Ping flood* envolveu a inclusão de parâmetros específicos, que foram: a utilização do argumento "-t" com a finalidade de manter o ping em execução indefinidamente; e a definição do tamanho máximo dos pacotes através do argumento "-l 65500", conforme ilustrado a figura 9.

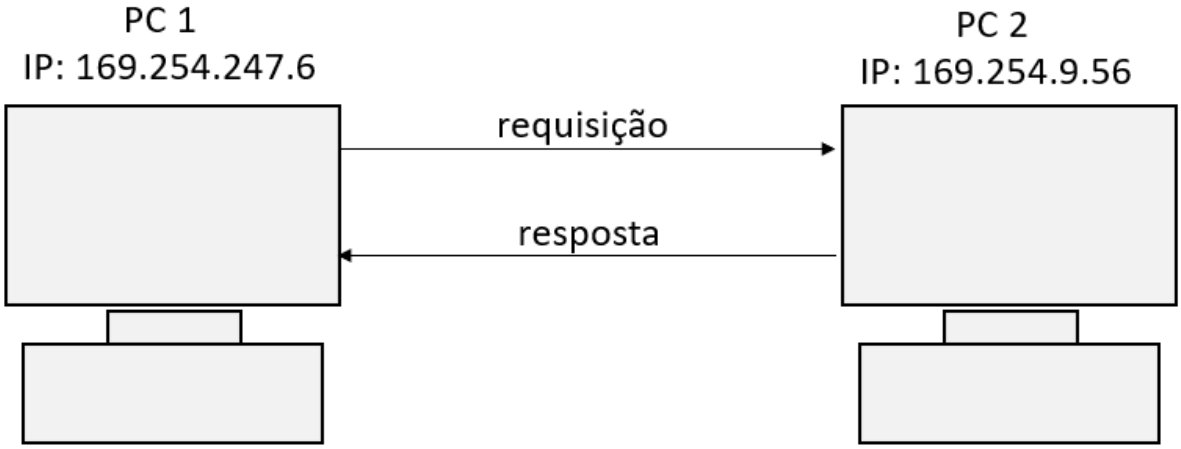
Figura 9 – Comandos para execução de *Ping flood* no Prompt de comando



Fonte: Capturada pelo autor.

Ataques de inundação de ping exploram uma vulnerabilidade do ICMP (*Internet Control Message Protocol*). A inundação é uma ferramenta de diagnóstico amplamente utilizada para detectar e solucionar problemas de rede (WILLIAM R., SANJEEV, 2021; PETANA et al., 2011). A Figura 10 ilustra o formato dos quadros de mensagens de requisição e resposta ao ping.

Figura 10 – Mensagens de requisição e resposta ao ping (CENTRALIZAR)



Requisição

Endereço de IP	Edereço de Destino	Função	Dados
169.254.247.6	169.254.9.56	8	

Endereço de IP	Edereço de Destino	Função	Dados
169.254.9.56	169.254.247.6	0	

Resposta

Fonte: Adaptado de Sanjeev et al. (2023)

Ao executar o *Ping flood* entre o PC 1 e o (PC 2), foi realizada a análise da influência do aumento no tráfego entre mestre e escravo. O RTT e o tempo de ciclo foram medidos nessa condição, também com 100 amostras. Os tempos foram medidos em cenários com a implementação da técnica de autenticação e sem a autenticação, visando a comparação no cenário de sobrecarga na rede. Esse processo proporcionou a análise do desempenho da rede HB Modbus, incluindo a latência temporal e a taxa de perda de pacotes, que são parâmetros essenciais para compreender o impacto da autenticação.

3.4 Utilização de TV Box para Simular Rede Modbus TCP com Mais Componentes e Verificação do Atraso no Processamento

O avanço da tecnologia resultou na proliferação de dispositivos eletrônicos, incluindo decodificadores utilizados para a recepção de televisão. Contudo, alguns desses dispositivos são empregados para fins ilícitos, como o acesso a conteúdo televisivo pago sem a devida autorização. Consequentemente, autoridades reguladoras, como a Receita Federal do Brasil, frequentemente apreendem esses decodificadores ilegais.

Com a finalidade de aumentar a implementação acadêmica, foram utilizados aparelhos TV Box apreendidos pela Receita Federal e autorizados para fins educacionais em parceria com o CEFET-MG, para simular uma rede Modbus TCP/IP contendo um maior número de componentes. Foram utilizadas quatro TV boxes, transformando-as em servidores Modbus, funcionando como escravos na rede, comunicando-se através de um switch e cabos Ethernet com um computador, atuando como Mestre.

As TV boxes utilizam o sistema operacional Armbian, apropriado para a finalidade empregada. Para estabelecer a rede entre o switch, o computador e as TV boxes, foram seguidas as etapas descritas a seguir:

1. **Instalação do Python e das Bibliotecas Necessárias:** Foram instalados o Python e as bibliotecas pip, numpy e bitstring com os seguintes comandos:

```
sudo apt-get install python3-numpy
sudo apt-get install python3-bitstring
```

2. **Execução dos Arquivos Modbus:** Após a instalação das bibliotecas, o terminal foi executado dentro da pasta onde estavam os arquivos Modbus Slave com e sem autenticação para comparação dos tempos de resposta.
3. **Configuração da Rede:** O switch foi conectado entre o computador e as TV boxes. Verificaram-se os IPs estabelecidos na rede e testou-se o programa para garantir a comunicação correta.
4. **Registro e Alteração de IP na TV Box:** Para configurar os IPs das TV boxes, foi editado o arquivo de interfaces de rede com o comando:

```
bash sudo nano /etc/network/interfaces
```

As configurações foram definidas da seguinte maneira:

```
auto eth0
allow-hotplug eth0
iface eth0 inet static
    address 192.168.56.X  # Endereço de IP
    netmask 255.255.255.0  # Máscara de Rede
    network 192.168.56.0   # Rede
```

Sendo que cada TV Box teve um IP diferente atribuído, da seguinte forma: Escravo 1 (192.168.56.2), Escravo 2 (192.168.56.3), Escravo 3 (192.168.56.4) e Escravo 4 (192.168.56.5).

5. **Reinício das TV Boxes:** As alterações foram salvas e as TV boxes foram reiniciadas para aplicar as novas configurações de rede.
6. **Verificação da Rede:** Após a reinicialização, foram realizados testes de ping para verificar se a rede foi estabelecida corretamente entre todos os componentes.
7. **Execução e Medição dos Tempos de Resposta:** Finalmente, os programas foram executados e os tempos de Round Trip Time (RTT) foram medidos com todos os componentes na rede. Foram comparados os tempos de resposta com e sem a técnica de autenticação.

Esta abordagem permitiu uma simulação eficaz de uma rede Modbus TCP com múltiplos componentes, possibilitando a análise dos atrasos no processamento e a comparação de desempenho com diferentes configurações de autenticação.

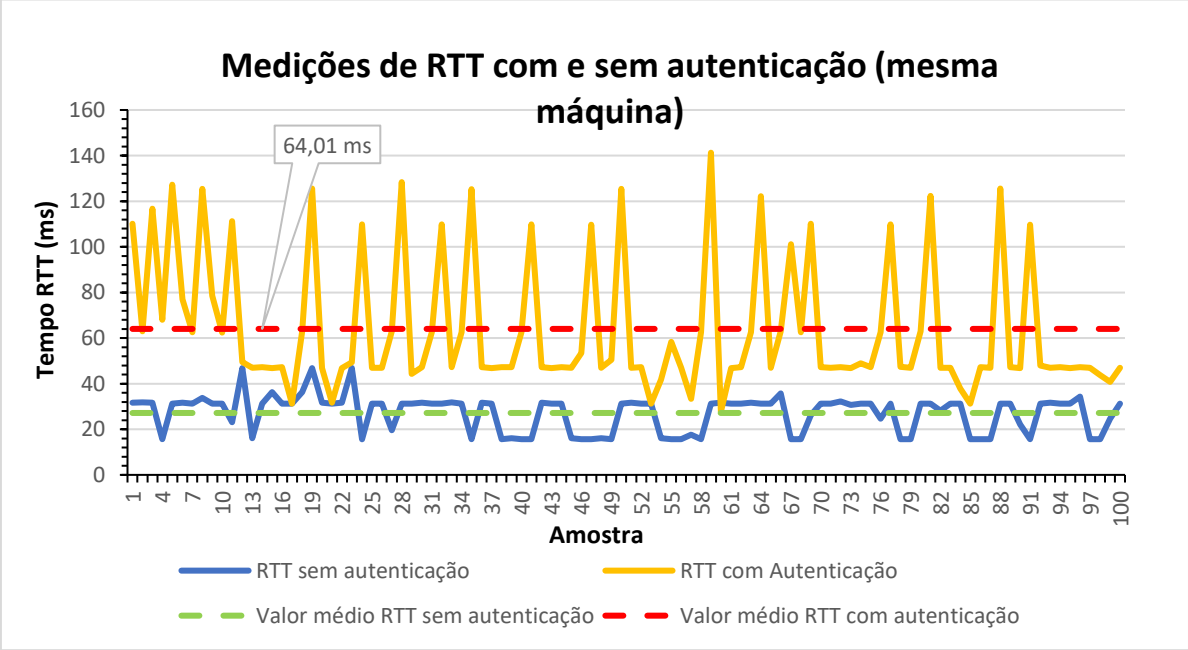
4 RESULTADOS

4.1 Impacto no tempo de transmissão com autenticação utilizando a mesma máquina

No contexto do primeiro teste de desempenho, com a intenção de mensurar o impacto do processo de autenticação na mesma máquina, o foco estava na avaliação do tempo de ida e volta (*Round Trip Time*) entre o envio de uma requisição e a recepção de uma resposta entre o mestre e o escravo da rede Modbus, considerando cenários com e sem autenticação.

Os resultados do teste revelaram um RTT médio de 64,01 ms em 100 amostras quando a autenticação estava presente, em comparação com um RTT médio de 27,15 ms quando a autenticação não era aplicada, ambos com o mesmo número de ciclos. A discrepância entre esses tempos médios forneceu uma estimativa do impacto da autenticação nos atrasos de processamento e transmissão dos dados HB-MP* numa mesma máquina, totalizando aproximadamente 36,86 ms (um aumento percentual de 135%). Esse aumento foi significativo, considerando tanto a magnitude do aumento quanto o próprio tempo envolvido. Os tempos mensurados estão graficamente representados no Gráfico 1.

Gráfico 1 – Medições de RTT na mesma máquina com e sem autenticação

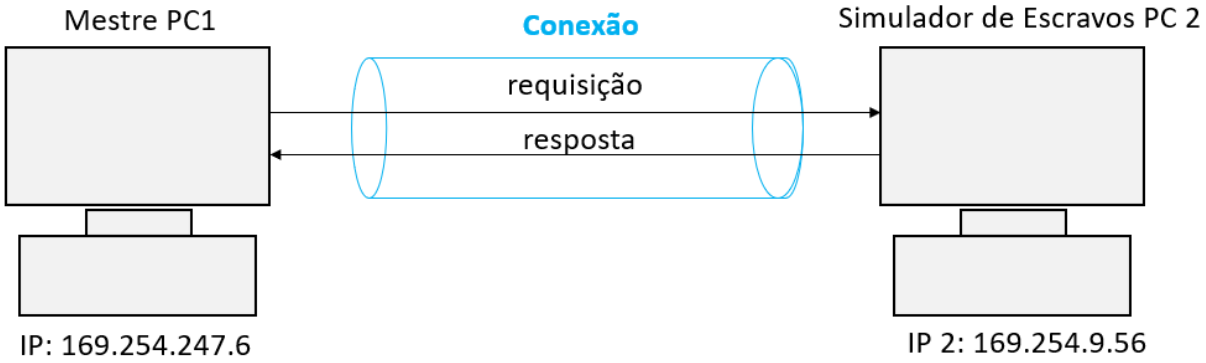


Fonte: Elaborada pelo autor

4.2 Impacto no tempo de transmissão com autenticação utilizando máquinas diferentes

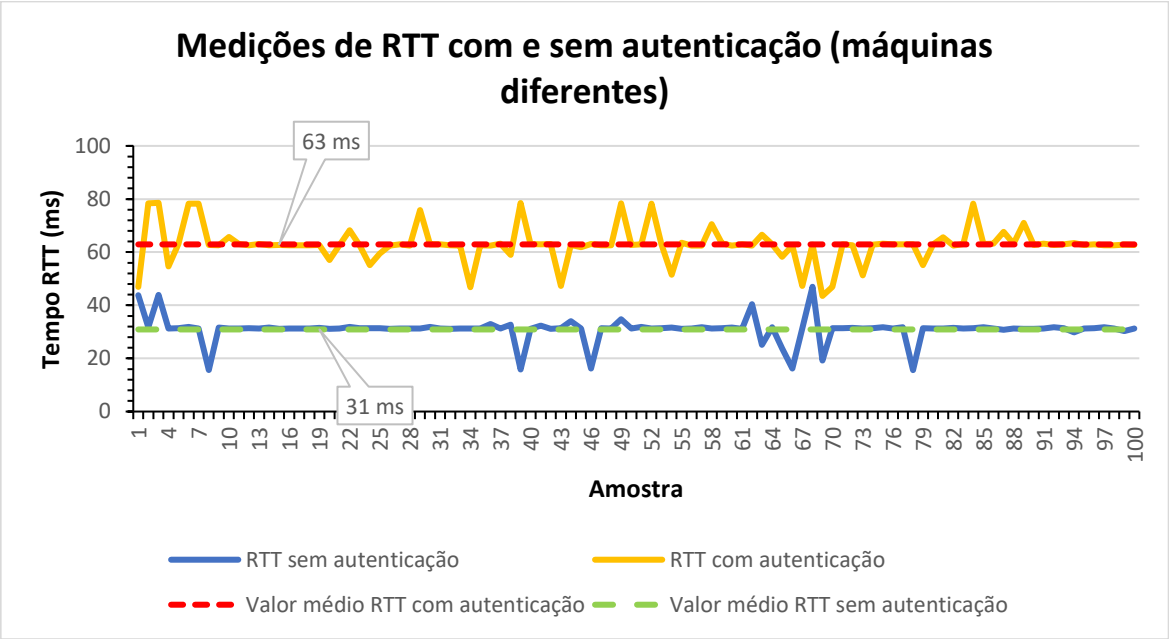
Semelhante ao teste de desempenho inicial da seção 4.1, dois computadores foram conectados, conforme ilustrado na Figura 11. Os resultados do teste revelaram um RTT médio de 63 ms em 100 amostras quando a autenticação estava presente, em comparação com um RTT médio de 31 ms quando a autenticação não era aplicada, ambos com o mesmo número de ciclos. O impacto da autenticação em máquinas diferentes foi de aproximadamente 32 ms (um aumento percentual de 103%). O Gráfico 2 representa os valores de tempos medidos.

Figura 11 – Rede Modbus estabelecida entre dois computadores



Fonte: Elaborada pelo autor

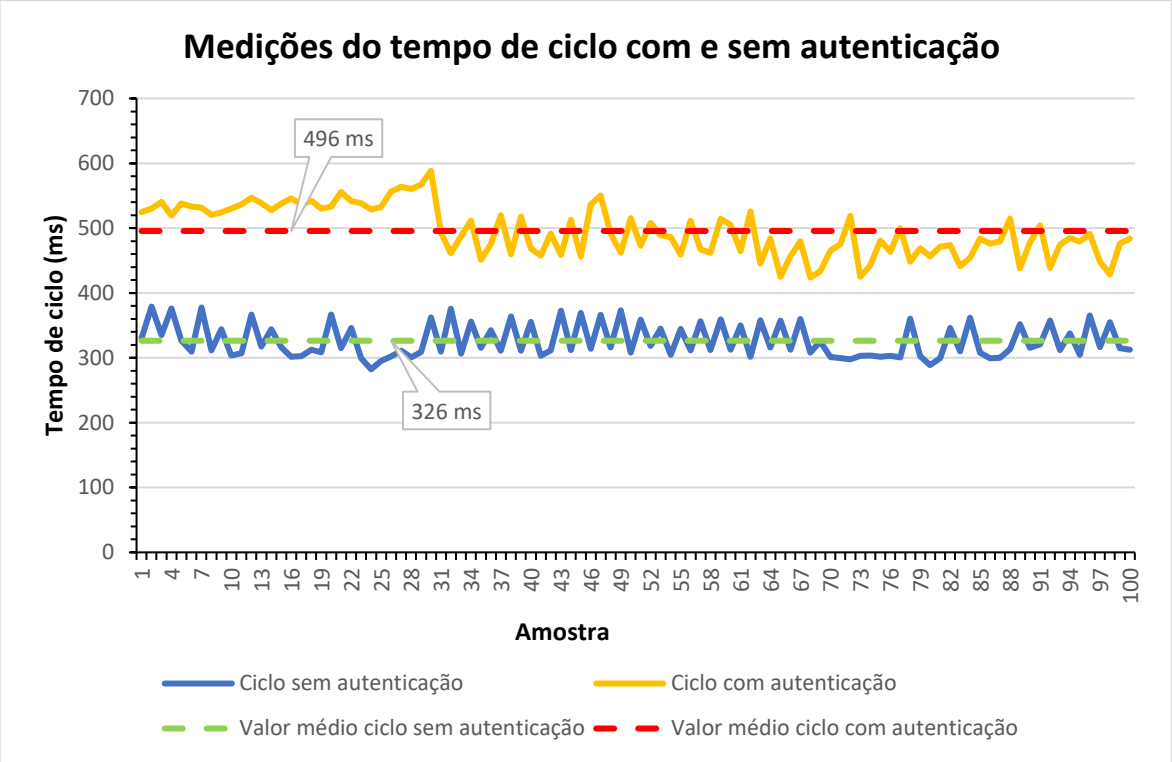
Gráfico 2 – Medições de RTT em máquinas diferentes com e sem autenticação



Fonte: Elaborada pelo autor

Para o teste em máquinas diferentes o tempo total do ciclo foi avaliado, e cada um dos 8 escravos (todos executados no PC 2, mas com novas conexões TCP sendo realizadas para cada um) recebeu e respondeu a uma requisição em cada ciclo. Durante a medição de 100 tempos totais de ciclo, a média observada com a autenticação foi de 496 ms e sem autenticação 326 ms (um aumento percentual de 52%). Os tempos mensurados estão graficamente representados no Gráfico 3.

Gráfico 3 – Medições do tempo de ciclo em máquinas diferentes com e sem autenticação

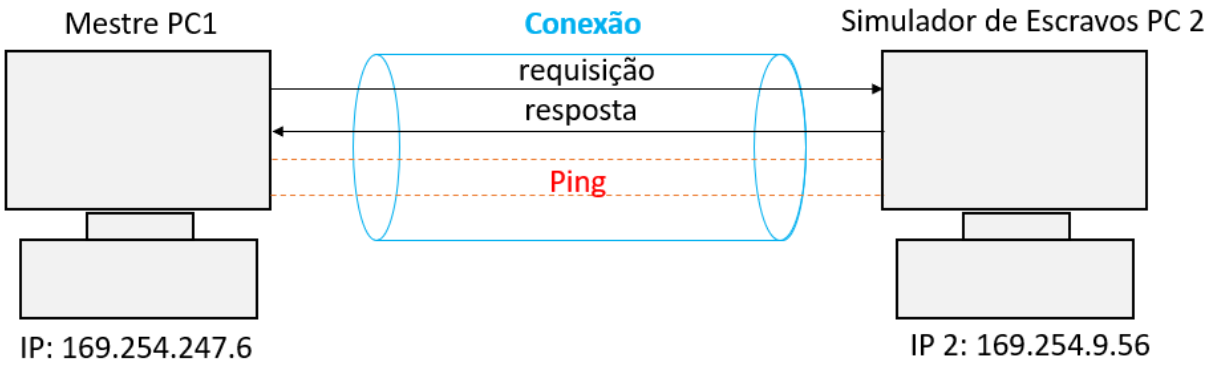


Fonte: Elaborada pelo autor

4.3 Testes de Sobrecarga Inicial em máquinas diferentes com inundação de ping

No contexto da sobrecarga da rede, buscou-se inicialmente determinar a resistência da camada de autenticação à inundação da rede. A metodologia empregada envolveu a aplicação de inundação ping (*Ping flood*), monitorando atentamente a autenticação para detectar possíveis pontos de falha ou degradação no desempenho. A Figura 12 ilustra o teste de sobrecarga inicial.

Figura 12 – Rede Modbus em máquinas diferentes com inundação de Ping



Fonte: Elaborada pelo autor

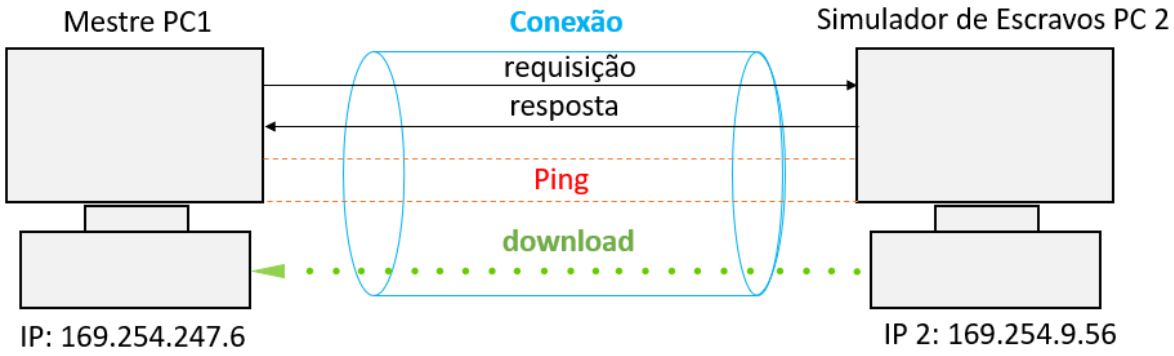
O teste de sobrecarga inicial não demonstrou efeitos adversos significativos na autenticação, sendo os valores medidos com inundação de ping bem próximos aos valores sem a inundação de ping, indicando uma resiliência inicial da camada de segurança em face de inundação de ping. A média observada com a autenticação foi de 496 ms e sem autenticação foi de 330 ms (valores bem próximos aos valores medidos anteriormente sem a inundação de ping).

Os resultados sugerem que a autenticação conseguiu lidar eficientemente com a sobrecarga moderada, preservando a integridade do processo de comunicação. Essa descoberta inicial é promissora, indicando não ter tanto impacto na transmissão em situações de tráfego moderado. No entanto, essa conclusão levanta a necessidade de uma análise mais aprofundada para compreender melhor os limites dessa resiliência e identificar possíveis cenários em que a autenticação pode se tornar um ponto crítico de falha.

4.4 Testes de Sobrecarga em máquinas diferentes com inundação de ping e transferência de arquivos

Em busca de uma compreensão mais abrangente da influência da autenticação em cenários de sobrecarga, o segundo teste foi realizado para explorar o desempenho da camada de segurança em condições mais desafiadoras. Replicando o método de sobrecarga inicial por meio inundação de ping, as cargas de tráfego foram incrementadas por meio de transferência de arquivos (download), mantendo a autenticação ativa, conforme ilustrado na Figura 13.

Figura 13 – Rede Modbus em máquinas diferentes com inundação de ping e sobrecarga de arquivos

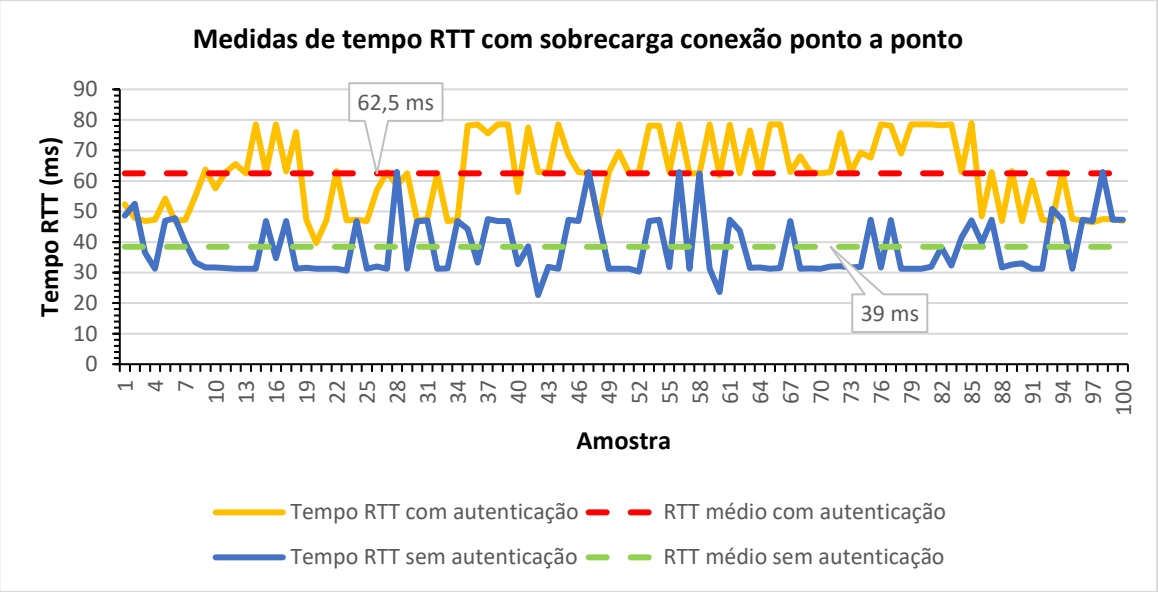


Fonte: Elaborada pelo autor

Este segundo conjunto de testes revelou uma degradação significativa no desempenho da rede, indicando que a autenticação, embora resiliente a sobrecargas moderadas, não é imune a condições com maior sobrecarga, por exemplo, transferência de arquivos extensos.

Os resultados do teste revelaram um RTT médio de 62,5 ms em 100 amostras quando a autenticação estava presente, em comparação com um RTT médio de 39 ms quando a autenticação não era aplicada, ambos com o mesmo número de ciclos. Desta forma, observou-se um aumento de aproximadamente 60% do valor RTT com autenticação em relação ao RTT sem autenticação. Entretando não houve diferenças significativas nos valores de RTT com e sem sobrecarga na rede mostrados no item 4.2. Os valores medidos estão representados no Gráfico 4.

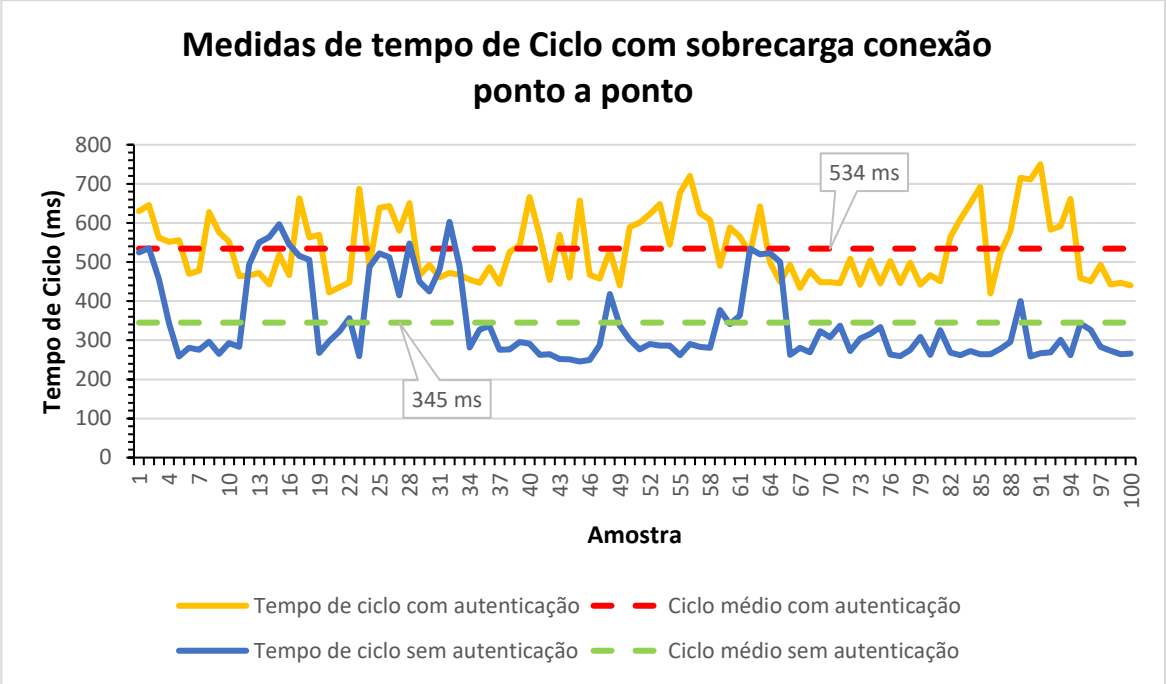
Gráfico 4 – Medidas de tempo RTT com sobrecarga na rede em conexão ponto a ponto



Fonte: Elaborada pelo autor

Durante a medição de 100 tempos totais de ciclo, a média observada com a autenticação foi de 534 ms e, sem a autenticação, 345 ms. Esse tempo de ciclo com autenticação e sobrecarga é 55% maior que o tempo de ciclo sem autenticação e sobrecarga (496 ms com autenticação e 326 ms sem autenticação, mostrados na seção 4.2). Os valores das medições dos tempos de ciclo estão representados no Gráfico 5.

Gráfico 5 – Medidas de tempo de ciclo com sobrecarga na rede em conexão ponto a ponto



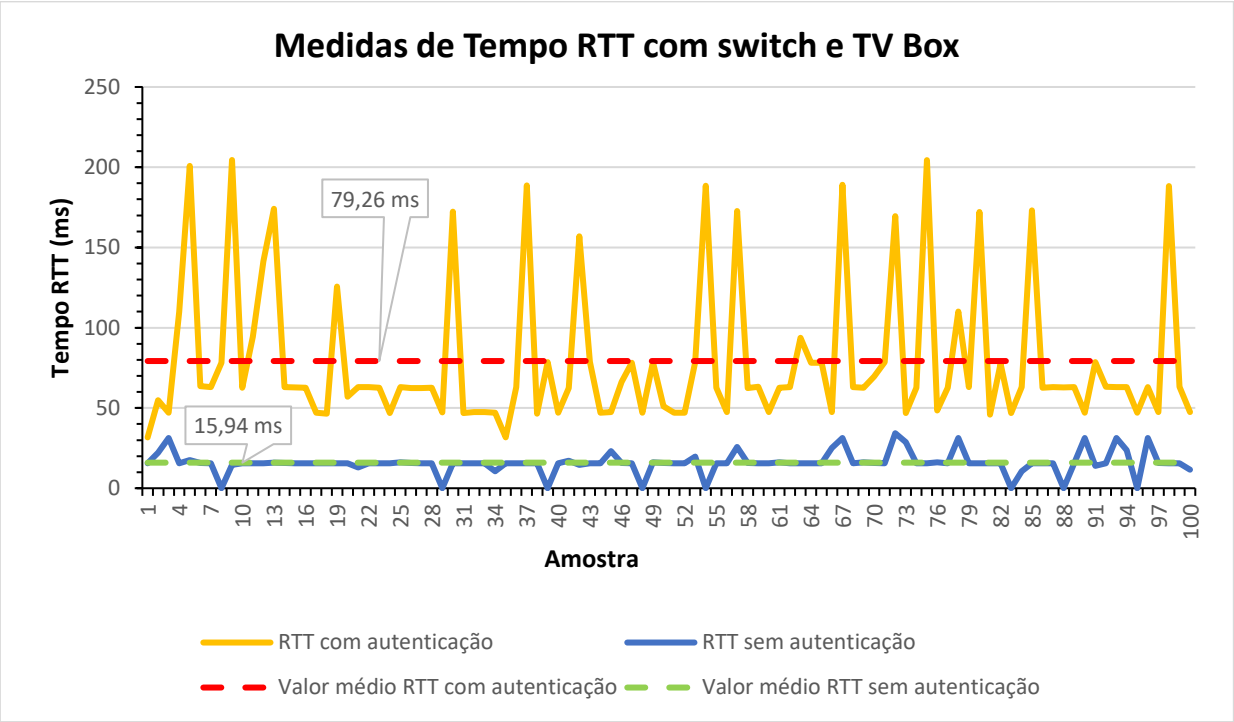
Fonte: Elaborada pelo autor

4.5 Impacto no tempo de transmissão com autenticação ao implementar mais componentes na rede (TV boxes)

Esta configuração visa uma maior aproximação de uma aplicação de rede Modbus TCP por estabelecer comunicação com um maior número de dispositivos, sendo que foram conectadas quatro TV boxes, atuando como dispositivos escravos e comunicando-se com o PC 1 através do switch via cabo Ethernet.

Para verificar o impacto no tempo de transmissão com o aumento do número de componentes na rede, primeiramente foram realizadas as medições dos tempos de uma TV box ligada com switch e o PC 1. Posteriormente, foram realizadas as medições dos tempos utilizando as quatro TV box, o switch e o PC 1. Os tempos mensurados estão graficamente representados no Gráfico 6 e no Gráfico 7.

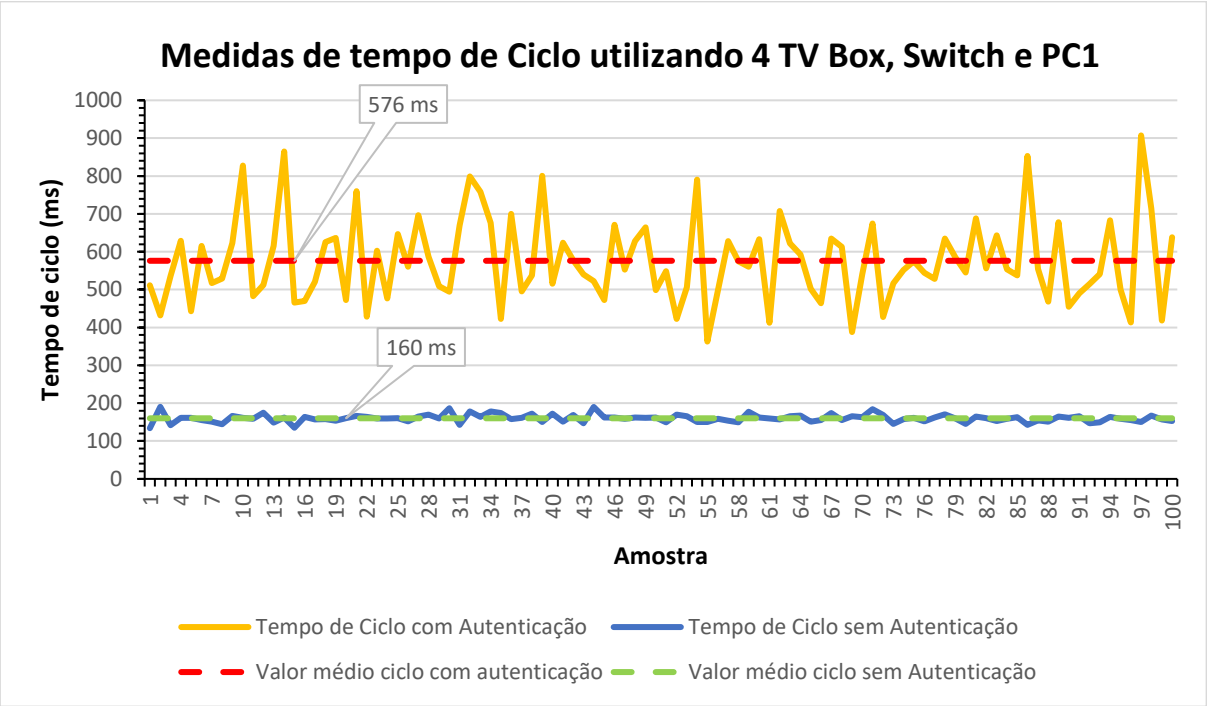
Gráfico 6 – Medições de tempo RTT utilizando PC 1, uma TV Box e switch



Fonte: Elaborada pelo autor

Os resultados do teste revelaram um RTT médio de 79,26 ms em 100 amostras quando a autenticação estava presente, em comparação com um RTT médio de 15,94 ms quando a autenticação não era aplicada. Desta forma, observou-se um aumento percentual de aproximadamente 397%.

Gráfico 7 – Medições de tempo de ciclo utilizando quatro TV Boxes, switch e PC 1



Fonte: Elaborada pelo autor

Os resultados do teste revelaram um tempo de ciclo médio de 576 ms em 100 amostras quando a autenticação estava presente, em comparação com um Tempo de ciclo médio de 160 ms quando a autenticação não era aplicada. Os tempos de ciclo foram feitos com quatro máquinas TV Box.

Com maior número de componentes na rede teve-se um aumento percentual de 260% no tempo de ciclo com autenticação. Desta forma, como esperado, pode-se confirmar que, quanto maior o número de componentes, maior será o impacto da autenticação para a transmissão de dados.

Os tempos mensurados considerando todos os testes estão representados na Tabela 1.

Tabela 1 – Tempo RTT e ciclo, considerando todos os testes de autenticação e sobrecarga na rede.

TESTES	Mesma máquina	Máquinas diferentes (8 escravos)	Sobrecarga de Ping	Sobrecarga de Ping e de Arquivos	TV Box e switch	4 TV Box e switch
RTT com autenticação (ms)	64,01	63	47	62,5	79,25	-
RTT sem autenticação (ms)	27,15	31	39	39	15,94	-
Ciclo com autenticação (ms)	-	496	496	534	-	576
Ciclo sem autenticação (ms)	-	326	330	345	-	160

Fonte: Elaborada pelo autor

A análise da rede Modbus TCP revelou a evolução do protocolo, desde sua implementação inicial até a introdução da autenticação HB-MP*. Ao implantar a autenticação, observamos um aumento significativo no tempo de transmissão, conforme evidenciado nos testes de desempenho realizados. Na mesma máquina, a autenticação resultou em um aumento percentual de 135% no Round Trip Time (RTT), indicando um impacto considerável nos atrasos de processamento e transmissão.

Ao estender os testes para máquinas diferentes, verificou-se que o RTT aumentou em 103% com a autenticação, destacando a influência da autenticação em ambientes mais representativos de redes industriais. Além disso, a análise do tempo total do ciclo demonstrou um aumento de 52%, enfatizando a relevância desses resultados em cenários práticos.

Os testes de sobrecarga com ataques de *Ping flood*, com e sem autenticação, em relação ao teste onde não houve ataques de *Ping flood*, apresentaram valores muito próximos comparando-se os tempos RTT e tempo de ciclo, também com e sem autenticação. No entanto, quando a rede foi sobrecarregada por transferência de arquivos, foi observado um impacto no tempo de transmissão de 8% (tempo de ciclo foi de 496 ms para 534 ms, ambos com sobrecarga na rede por transferência de arquivos e com autenticação).

Finalmente, o impacto da autenticação ao adicionar mais componentes à rede foi avaliado. A conexão de quatro TV boxes resultou em um RTT médio de 79,26 ms com autenticação, em comparação com 15,94 ms sem, representando um aumento percentual de 397%. O tempo de ciclo médio também apresentou um aumento de 260%. Esses dados ressaltam a importância de considerar o impacto da autenticação em redes com alta demanda de tráfego, pois o aumento no número de componentes acentua a latência e a degradação do desempenho da comunicação.

Finalmente, o impacto da autenticação ao adicionar mais componentes à rede foi avaliado. A conexão de quatro TV boxes resultou em um RTT médio de 79,26 ms com autenticação, em comparação com 15,94 ms sem, representando um aumento percentual de 397%. O tempo de ciclo médio também apresentou um aumento de 260%. Esses dados ressaltam a importância de considerar o impacto da autenticação em redes com alta demanda de tráfego, pois o aumento no número de componentes acentua a latência e a degradação do desempenho da comunicação.

5 CONCLUSÃO

A automação industrial, impulsionada por avanços tecnológicos e pela crescente complexidade das operações, demanda soluções que garantem a velocidade, segurança e eficiência na transmissão de dados. E esses três elementos cruciais para o sucesso operacional em processos industriais.

O contexto contemporâneo das redes industriais é caracterizado pela priorização da segurança, um imperativo incontestável na proteção de ativos valiosos e na garantia da continuidade operacional. A introdução da autenticação HB-MP* no protocolo Modbus TCP representa um passo significativo na resposta a essa demanda, proporcionando uma camada adicional de segurança em um ambiente propenso a ameaças diversas.

No decorrer deste trabalho, foi explorada a influência da autenticação HB-MP* no desempenho da rede Modbus TCP em diferentes cenários. Inicialmente destacando a crescente importância da automação industrial, que visam otimizar processos, melhorar a qualidade dos produtos e aumentar a produtividade para atender às demandas do mercado.

Os resultados obtidos destacam a importância crítica da autenticação em redes industriais, onde a segurança é essencial. Embora a autenticação HB-MP* tenha se mostrado eficiente em condições normais e moderadas de sobrecarga, é fundamental considerar suas limitações em situações com maior sobrecarga na rede.

Considerando esses resultados, é crucial continuar explorando abordagens aprimoradas de autenticação e estratégias para lidar com cenários de sobrecarga mais intensos. Além disso, a implementação prática da autenticação deve ser cuidadosamente ponderada em relação aos benefícios de segurança proporcionados em comparação com os possíveis impactos no desempenho da rede.

Este trabalho fornece uma base para futuras pesquisas na área de segurança em redes industriais, contribuindo para o avanço do conhecimento e práticas que buscam equilibrar eficácia e desempenho nessas redes cruciais para a automação industrial.

6 REFERÊNCIAS

ALOTAIBI, A. M. et al. Security issues in protocols of TCP/IP model at layers level. International Journal of Computer Networks and Communications Security, v. 5, n. 5, p. 96–104, 2017.

ASEERI, Aisha; BAMASAG, Omaimah. Achieving protection against man-in-the-middle attack in HB family protocols implemented in RFID tags. International Journal of Pervasive Computing and Communications, v. 12, n. 3, p. 375-390, 2016.

BISHOP, R. H. **The Mechatronics Handbook**. Austin, Texas: CRC Press LLC , 2002.
BRANQUINHO, M. A. et al. **Segurança de Automação Industrial e SCADA**. Rio de Janeiro: Elsevier, 2014.

Boutin, J.-I. (2017). Dragonfly 2.0: the resurgence of a cyber-espionage group. *WeLiveSecurity*. Disponível em ESET Article on Dragonfly 2.0.

CHEMINOD, M. et al. Performance evaluation and modeling of an industrial application-layer firewall. **IEEE Transactions on Industrial Informatics**, v. 14, n. 5, p. 2159–2170, 2018.

CHIEN, E., FALLIERE, N., & O MURCHU, L. (2011). "W32.Stuxnet." I**EEE Security & Privacy**. DOI: 10.1109/MSP.2011.154.

FAGUNDES, F. D. **Segurança em Redes Industriais: Aplicação da técnica de autenticação HB-MP* em rede Modbus**. Orientador: Ernane Antônio Alves Coelho. 2022. Tese de doutorado (Pós-graduação) – Faculdade de Engenharia Elétrica, Universidade Federal de Uberlândia, Uberlândia, 2022

GALLOWAY, B.; HANCKE, G. P. Introduction to industrial control networks. **IEEE Communications Surveys & Tutorials**, v. 15, n. 2, p. 860–880, 2013

GINTER, A., LANGNER, R., et al. (2013). Seven Myths of Industrial Control Systems Security. **IEEE Security & Privacy**, DOI: 10.1109/MSP.2013.36.

KRAWCZYK, Hugo; BELLARE, Mihir; CANETTI, Ran. **HMAC: Keyed-Hashing for Message Authentication.** [S.l.], February 1997. http://www.rfc-editor. org/rfc/rfc2104.txt. Disponível em: .

HUITSING, P. et al. Attack taxonomies for the modbus protocols. International Journal of Critical Infrastructure Protection, Elsevier, v. 1, p. 37–44, 2008.

HOPPER, N. J.; BLUM, M. Secure human identification protocols. In: BOYD, C. (Ed.). Advances in Cryptology — ASIACRYPT 2001. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001. p. 52–66. ISBN 978-3-540-45682-7.

LANGNER, R., Stuxnet: Dissecting a cyberwarfare weapon[J]. **IEEE Security and Privacy**, 2011. 9(3): p. 49-51.

LUGLI, A. B.; SANTOS, M. M. D. **Redes Industriais:** Características, Padrões e Aplicações. São Paulo: Érica, 2014.

MORAES, C. C.; CASTRUCCI, L. **Engenharia de Automação Industrial**. Rio de Janeiro: LTC, 2007.

MODBUS ORG. **Modbus application protocol specification v1.1b3**. Hopkinton, EUA: Modbus Organization, 2012.

MODBUS ORG. **Modbus/TCP Security**: Protocol specification. Hopkinton, EUA: Modbus Organization, 2018.

NEVES, G.; SAUER, F. **Segurança em Redes Industriais. Análise vulnerabilidades, gerência de ataques e erros, evitando catástrofres**. Rio de Janeiro: [s.n.], 2011.

PETANA et al. “TCP SYN-Based DDoS Attack on EKG Signals Monitored via a Wireless Sensor Network.” **Security and Communication Networks**, vol. 4, no. 12, 2011, pp. 1448–1460., doi:10.1002/sec.275

PELLEGRINI, J. C. **Introdução à criptografia e seus fundamentos**. [S.l.]: [s.n.], 2018.

Perry S. Marshall. (2016). "Industrial Ethernet, 2nd Edition." **ISA International Society of Automation**. ISBN: 978-1941546888.

REYNDERS, D.; MACKAY, S.; WRIGHT, E. **Practical Industrial Data Communications. Best Practice Techniques**. Burlington: Elsevier, 2005.

RIBEIRO, M. A. **Automação Industrial**. Salvador: Tek Treinamento & Consultoria Ltda, 1999.

SLOWIK, J. (2018). A Deep Dive into TRITON Malware. **SANS Institute**. Disponível em SANS Technical Article on TRITON.

Schneider Automation. Modbus messaging on tcp/ip implementation guide v1. 0b. **MODBUS Organization, last accessed June**, p. 46, 2022

SENAI, **Redes Industriais**, Rio Grande do Sul: SENAI – Departamento Nacional, 2014.

Symantec Security Response. (2014). "Dragonfly: Western Energy Companies Under Sabotage Threat." Disponível em: Symantec Report on Dragonfly.

VOLKOVA, A. et al. Security challenges in control network protocols: A survey. **IEEE Communications Surveys & Tutorials**, IEEE, v. 21, n. 1, p. 619–639, 2019.

WILLIAM R., SANJEEV K., “**Evaluation of CentOS performance under IoT based DDoS Security Attacks**,” proceedings of 3rd International Conference on Data Intelligence and Security (ICDIS), pp. 64-70, January 2021.

CÓPIA DO TRABALHO Nº 152/2024 - DELMAX (11.57.05)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 18/09/2024 17:23)
FREDERICO DUARTE FAGUNDES
PROFESSOR ENS BASICO TECN TECNOLOGICO
DELMAX (11.57.05)
Matrícula: ###071#5

Visualize o documento original em https://sig.cefetmg.br/documentos/ informando seu número: ***152****, ano:* ***2024****, tipo:* ***CÓPIA DO TRABALHO****, data de emissão:* ***18/09/2024*** *e o código de verificação:* ***fad6bf9d9b***