ISSN: 2319-0124
josif 2023
15ª JORNADA CIENTÍFICA E TECNOLÓGICA
12º SIMPÓSIO DE PÓS-GRADUAÇÃO
DO IFSULDEMINAS
REALIZAÇÃO INSTITUTO FEDERAL Sul de Minas Gerais
APOIO FAPEMIG CNPq

ESTUDO DE MÉTODOS PARA PROVIMENTO DE SEGURANÇA E FLUIDEZ NA TRANSMISSÃO DE DADOS NO CONTEXTO DA INTERNET DAS COISAS

Renan R. RUIVO[1]; Matheus G. VILAS BOAS[2]

RESUMO

A crescente preocupação com a segurança das redes na Internet das Coisas (IoT) é motivada pelo aumento exponencial do número de dispositivos conectados e pela transmissão em larga escala de volumes cada vez maiores de dados. Esse cenário representa um desafio significativo, uma vez que a vasta quantidade de dispositivos e a constante troca de informações tornam as redes IoT altamente vulneráveis a ataques cibernéticos e violações de privacidade.

O artigo apresenta abordagens para aprimorar a segurança na IoT, como a ofuscação do tráfego de rede (exemplo: método Mitra) e a detecção de vulnerabilidades através de técnicas de aprendizagem de máquinas (exemplo:método MANDRAKE). O Protocolo da IoT contribui para reduzir o tráfego e melhorar a eficiência energética. A tecnologia SDN fortalece a segurança e análise de dados. A combinação dessas abordagens melhora a segurança na IoT, exigindo práticas seguras dos usuários finais. Este estudo avança o conhecimento sobre segurança na IoT e sugere soluções eficientes. A colaboração entre segurança da informação e redes é essencial para enfrentar desafios de segurança na IoT.

Palavras-chave:
seguranças de redes; métodos de segurança; IoT

1. INTRODUÇÃO

Com o avanço da Internet das Coisas (IoT), a segurança da rede é crucial. Com milhões de dispositivos conectados, a vulnerabilidade aumenta. Isso requer medidas robustas, como senhas fortes e criptografia. Usuários devem ser conscientizados dos riscos e incentivados a práticas seguras, como atualizações regulares e senhas fortes. O crescimento rápido da IoT torna a segurança dos dados urgente. Prevê-se aumento de dispositivos conectados. É vital entender melhor os métodos de segurança para garantir a privacidade. Este estudo contribui para soluções mais seguras na transmissão de dados, permitindo aproveitar os benefícios da IoT sem comprometer a segurança. Isso avança o conhecimento em segurança de dados na IoT.

Objetivos incluem pesquisa de métodos, focando em segurança na IoT; estudar o Protocolo IoT; aprender detecção de vulnerabilidades por aprendizado de máquina (ex:método MANDRAKE); explorar ofuscação de tráfego (ex: método Mitra); entender arquitetura SDN; propor uso conjunto de técnicas estudadas.

2. FUNDAMENTAÇÃO TEÓRICA

A seguir, são apresentados os artigos encontrados por meio das pesquisas bibliográficas.

No trabalho de, Brezolin et al. (2022) o método MANDRAKE é apresentado, usando análise

[1].Renan Ruivo Anselmo Autor IFSULDEMINAS – Campus Inconfidentes. E-mail: renan.ruivo@alunos.ifsuldeminas.edu.br
[2]Matheus Guedes Vilas Boas Orientador, IFSULDEMINAS – Campus Inconfidentes. E-mail: matheus.vilasboas@ifsuldeminas.edu.br

de tráfego e aprendizado de máquina para detectar vulnerabilidades em casas inteligentes. Outro estudo, "*IoT Devices Recognition through Network Traffic Analysis*", de SHAHID, Mustafizur R et al.(2018) explora o reconhecimento de dispositivos IoT via análise de tráfego de rede. Investiga como padrões únicos de tráfego de dispositivos IoT podem ser usados para identificação de vulnerabilidades.

Além disso, Madureira et al. (2020) introduzem o Protocolo IoTP, reduzindo tráfego e aumentando escalabilidade na IoT com agregação de dados. Seguindo no sentido de agregação de dados, o estudo de Karlsson et al. (2009) estudou o resultado da agregação de dados no desempenho do protocolo TCP. Outra tecnologia para segurança é discutida no trabalho de Prates et al. (2018) explorando o uso da tecnologia SDN (*Software-Defined Networking*) para fortalecer a segurança e análise de dados na IoT. O SDN é uma abordagem inovadora que permite gerenciar e controlar redes de forma centralizada, separando o plano de controle do plano de dados. Uma outra técnica apresentada no trabalho de dos Santos et al. (2022), é a técnica Mitra para gerar tráfego falso e melhorar a privacidade na segurança de redes IoT. Por fim, o trabalho de Pinheiro, Antônio J. et al(2020) discute a ofuscação de dados e a utilização do SDN para controle dos dados.

3. MATERIAL E MÉTODOS

Este artigo se trata de uma revisão bibliográfica e foi utilizado como método de pesquisa o site do Simpósio Brasileiro de Computação, iee.org e o Google Scholar para buscar artigos publicados relacionados ao tema. As palavras-chave utilizadas foram "segurança de rede IoT", "privacidade em rede IoT" e "fluidez em redes IoT" e respectivamente em inglês.

4. RESULTADOS E DISCUSSÃO

O artigo apresenta uma análise abrangente de diversas abordagens para aprimorar a segurança e a privacidade na Internet das Coisas (IoT). As revisões literárias abordam desde a proteção da privacidade no tráfego de rede até a detecção de vulnerabilidades, passando pela redução do tráfego e análise de requisitos de segurança. Todas essas abordagens desempenham um papel crucial na garantia da confiança e proteção dos dispositivos conectados na IoT.

Uma das estratégias discutidas é o método MANDRAKE, uma abordagem para a detecção de vulnerabilidades na IoT. Esse método utiliza análise do tráfego de rede e técnicas de aprendizado de máquina para identificar vulnerabilidades, como a transferência de dados sem criptografia. Os resultados obtidos demonstram uma alta precisão de detecção, chegando a 99% na criptografia do tráfego, fortalecendo a segurança na IoT.

Outro estudo, "*IoT Devices Recognition through Network Traffic Analysis*", explora o reconhecimento de dispositivos IoT via análise de tráfego de rede. Investiga como padrões únicos

de tráfego de dispositivos IoT podem ser usados para identificação. A análise de tráfego é combinada com técnicas de reconhecimento de padrões e aprendizado de máquina para melhorar a eficiência. O estudo destaca sua relevância para otimização e segurança nas redes IoT, oferecendo percepções valiosas sobre identificação de dispositivos e ameaças.

Outra estratégia em discussão é o Protocolo da Internet das Coisas (IoTP), que tem como objetivo a redução do tráfego de rede e o aumento da eficiência energética na comunicação da IoT. Este protocolo utiliza técnicas de agregação de dados para consolidar pacotes, diminuindo a quantidade de informações dispensáveis transmitidas pela rede. Os resultados da pesquisa ressaltam uma melhoria de 78% na rede com a implementação do IoTP, trazendo benefícios para o consumo de energia e a escalabilidade do sistema.

A fim de ressaltar a importância da agregação de dados, o estudo conduzido por Karlsson et al. (2009) analisou os impactos dessa técnica no desempenho do protocolo TCP. Os resultados alcançados destacam um aumento significativo de até 73% no desempenho geral do TCP com a adoção da técnica de agregação. Além desse avanço, foram observadas melhorias na capacidade global, na taxa de transferência e na eficiência do protocolo. Como resultado direto, também ocorreu uma redução no atraso da transmissão fim a fim.

Uma tecnologia muito importante para garantir a segurança é a tecnologia de Rede Definida por Software (SDN) como uma ferramenta para fortalecer a segurança e a análise de dados na IoT. A SDN oferece uma abordagem centralizada para gerenciar e controlar redes, possibilitando a implementação de medidas avançadas de defesa contra ameaças e a análise em tempo real dos dados. A colaboração entre os campos de segurança da informação e redes de comunicação é enfatizada como fundamental para enfrentar os desafios de segurança na IoT.

Por fim, destaca-se o método de ofuscação do tráfego de rede, que visa aprimorar a privacidade dos usuários na IoT. O uso da técnica de ofuscação Mitra é destacado como uma forma de gerar tráfego falso e dificultar a identificação dos dispositivos. Os resultados obtidos evidenciam a eficácia da ofuscação do tráfego, com uma redução de até 42% na precisão de identificação dos dispositivos.

O artigo "*Adaptive Packet Padding for Smart Home Networks: Balancing Privacy and Performance*" aborda a importância da ofuscação de dados e do uso do método SDN. Ele propõe uma abordagem adaptativa que ajusta dinamicamente o preenchimento de pacotes com base na atividade da rede doméstica. Isso equilibra privacidade e desempenho, especialmente em casas inteligentes com tráfego variável. O papel crucial do SDN permite essa adaptação dinâmica, resultando em proteção eficaz da privacidade em redes residenciais inteligentes.

O artigo sugere que a utilização conjunta de todos os meios apresentados possa aprimorar a segurança de uma rede IoT, uma vez que cada um deles desempenha um papel específico na

garantia da segurança.

5. CONCLUSÃO

A segurança nas redes da IoT é essencial devido ao crescente número de dispositivos conectados e ao aumento da transmissão de dados. O artigo apresentou abordagens para melhorar a segurança e a privacidade, incluindo ofuscação de tráfego (ex: método Mitra), detecção de vulnerabilidades (método MANDRAKE), e redução do tráfego por meio do Protocolo IoT.

A tecnologia SDN também é mencionada para fortalecer a segurança e análise de dados na IoT. Combinar essas abordagens melhora a segurança da rede IoT, mas é crucial que os usuários adotem práticas seguras.

Esse estudo avança o conhecimento na segurança da IoT, fornecendo *insights* para soluções eficientes e seguras na transmissão de dados. A colaboração entre segurança da informação e redes é vital para enfrentar os desafios de segurança de uma rede IoT.

REFERÊNCIAS

BREZOLIN, Uelinton Q. et al. Um Método para Detecção de Vulnerabilidades Através da Análise do Tráfego de Rede IoT. In: Anais do XL Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. SBC, 2022. p. 447-460.

DOS SANTOS, Bruna V. et al. Um Método de Ofuscação para Proteger a Privacidade no Tráfego da Rede IoT. In: Anais do XL Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. SBC, 2022. p. 126-139.

MADUREIRA, André Luiz; ARAÚJO, Francisco Renato; SAMPAIO, Leobino. Um Protocolo IoT para Redução de Tráfego em Redes de Plano de Dados Programáveis. In: Anais do XXXVIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. SBC, 2020. p. 826-839.

PINHEIRO, Antônio J. et al. Adaptive packet padding approach for smart home networks: A tradeoff between privacy and performance. IEEE Internet of Things Journal, v. 8, n. 5, p. 3930-3938, 2020.

PRATES JR, Nelson G. et al. Ameaças de segurança, defesas e análise de dados em IoT baseada em SDN. Sociedade Brasileira de Computação, 2018.

SHAHID, Mustafizur R. et al. IoT devices recognition through network traffic analysis. In: 2018 IEEE international conference on big data (big data). IEEE, 2018. p. 5187-5192.

KARLSSON, Jonas; KASSLER, Andreas; BRUNSTROM, Anna. Impact of packet aggregation on TCP performance in wireless mesh networks. In: 2009 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks & Workshops. IEEE, 2009. p. 1-7