UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE CIÊNCIAS

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

FELIPE CAVALCANTE MONTEIRO

DPNETTRAFFIC - COMPARTILHAMENTO DE DADOS DE TRÁFEGO DE REDE UTILIZANDO PRIVACIDADE DIFERENCIAL

FORTALEZA

2023

FELIPE CAVALCANTE MONTEIRO

DPNETTRAFFIC - COMPARTILHAMENTO DE DADOS DE TRÁFEGO DE REDE UTILIZANDO PRIVACIDADE DIFERENCIAL

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação do Centro de Ciências da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Ciência da Computação. Área de Concentração: Banco de Dados.

Orientador: Prof. Dr. Javam de Castro Machado.

FORTALEZA

2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

M776d Monteiro, Felipe Cavalcante.
DPNETTRAFFIC - Compartilhamento de Dados de Tráfego de Rede Utilizando Privacidade Diferencial / Felipe Cavalcante Monteiro. – 2023.
75 f. : il. color.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Programa de Pós-Graduação em Ciência da Computação, Fortaleza, 2023.
Orientação: Prof. Dr. Javam de Castro Machado.

1. Privacidade de Dados. 2. Privacidade Diferencial. 3. Tráfego de Redes. 4. Pós-Processamento. I. Título.

CDD 005

FELIPE CAVALCANTE MONTEIRO

DPNETTRAFFIC - COMPARTILHAMENTO DE DADOS DE TRÁFEGO DE REDE UTILIZANDO PRIVACIDADE DIFERENCIAL

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação do Centro de Ciências da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Ciência da Computação. Área de Concentração: Banco de Dados.

Aprovada em: 11/08/2023.

BANCA EXAMINADORA

Prof. Dr. Javam de Castro Machado (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. João Paulo Pordeus Gomes
Universidade Federal do Ceará (UFC)

Prof. Dr. Paulo Antonio Leal Rego
Universidade Federal do Ceará (UFC)

Prof. Dr. Victor Aguiar Evangelista de Farias
Universidade Federal do Ceará (UFC)

AGRADECIMENTOS

Durante toda minha vida, sempre ouvi que a pesquisa acadêmica é um caminho solitário. No entanto, agora percebo o quão equivocada essa afirmação é. Se não fosse por essa rede de amizade, colaboração e suporte, esta seção em particular não existiria e, mais importante ainda, o trabalho que apresento não teria sido possível.

Agradeço primeiramente aos meus pais, Aldir e Aldeniza, por seu amor, incentivo e apoio incondicional. Também agradeço minha irmã, Natália e meu sobrinho João Victor. Peço desculpas pelas minhas ausências e agradeço por compreenderem e apoiarem minhas escolhas. Vocês são minha motivação constante e me lembram do valor de ter uma família tão maravilhosa.

Ao Daniel Sampaio, por estar sempre ao meu lado no dia a dia. Sua presença constante e apoio têm sido fundamentais ao longo de todo este processo. Compartilhando não apenas as alegrias e os carnavais, mas também dividindo as dores. Obrigado por estar presente e por tornar essa jornada mais leve e significativa.

Ao Felipe Timbó, amigo de longa data e parceiro de pesquisa e trabalho. Sempre fornecendo suporte, orientação e encorajamento ao longo de todo o processo.

Aos amigos cearenses, mineiros e pernambucanos mais amados em linha reta, Camille Soares, Ticiane Morais, Andrea Araújo, Eugênia Cabral, João Cumaru, Aída Araújo, Lara Martins e Marina Pordeus. Gonzaguinha já dizia: *"É tão bonito quando a gente entende que a gente é tanta gente onde quer que a gente vá"*.

Aos colegas de trabalho e ao time do LDE. Em especial Geisiane França, Lucas Montesuma, Julio Oliveira, Israel Vidal e Tiago Nascimento. Mesmo nos momentos mais desafiadores, vocês estiveram ao meu lado, inclusive nas madrugadas de trabalho intenso. Agradeço por compartilharem não apenas o ambiente de trabalho, mas também risadas, desafios e conquistas.

Ao parceiro de pesquisa, trabalho e estádio Iago Chaves. Obrigado pela dedicação, disponibilidade e aos intermináveis devaneios sobre a vida, trabalho e pesquisa. Eles foram fundamentais ao longo dessa jornada.

Ao meu orientador, professor, chefe e amigo, Javam Machado. Agradeço por sua paciência, parceria e dedicação. Nossos diálogos enriquecedores e os momentos em que tomamos café juntos foram fundamentais para o sucesso deste trabalho e do projeto LDE. Agradeço por acreditar em mim e por todo o trabalho árduo que realizamos juntos tanto na pesquisa como no LSBD.

À banca que me acompanha desde o início deste trabalho, Prof. Victor Farias, Prof. João Paulo e mais recentemente o Prof. Paulo Rego. Agradeço pelas valiosas discussões, orientações, ensinamentos e esclarecimento de dúvidas. Obrigado por compartilharem seus conhecimentos e serem fontes de inspiração.

Por fim, agradeço também ao LSBD e aos colegas de pesquisa, Serafim, Ítalo, Paulo, Daniel, Falcão e Edvar. Em especial Malu Maia, André Luís e Eduardo Rodrigues por compartilharem suas valiosas experiências, conhecimentos e apoio ao longo de todo esse processo.

“O correr da vida embrulha tudo, a vida é assim:
esquenta e esfria, aperta e daí afrouxa,
sossega e depois desinquieta.
O que ela quer da gente é coragem."

(Rosa. Guimarães, 1956)

RESUMO

Dados de tráfego de redes são extremamente valiosos e desempenham um papel fundamental em uma variedade de aplicações. Essas informações são coletadas por diferentes entidades, como provedores de serviço de internet (ISPs), que geralmente compartilham ou comercializam esses dados com entidades externas. No entanto, o compartilhamento desses dados pode potencialmente comprometer a privacidade das pessoas cujas informações estão contidas neles. Com o objetivo de abordar essa preocupação com a privacidade, propomos uma nova técnica chamada *DPNetTraffic*. Essa proposta utiliza o conceito de privacidade diferencial, que consiste em adicionar um nível controlado de ruído aos dados originais. Dessa forma, a privacidade de informações sobre tráfego de rede contidas nos dados é preservada, pois os dados compartilhados não revelam informações específicas e identificáveis sobre eles. A abordagem *DPNetTraffic* se destaca por sua eficiência em preservar a privacidade de informações dos dados de tráfego de rede. Comparada a outras técnicas que também adotam a privacidade diferencial, os resultados experimentais demonstraram que ela introduz menos ruído nos dados. Isso significa que é possível realizar análises e obter informações úteis dos dados compartilhados, ao mesmo tempo em que se protege a privacidade dos indivíduos envolvidos. A utilização do *DPNetTraffic* no compartilhamento de dados de tráfego de rede representa um avanço significativo no equilíbrio entre a utilidade dos dados e a proteção da privacidade dos usuários. Essa abordagem tem o potencial de ser adotada por entidades que coletam e compartilham dados de tráfego de rede, oferecendo uma solução confiável e eficaz para mitigar os riscos de violações de privacidade. Em relação aos resultados específicos de comparação com o *baseline*, a abordagem proposta, denominada *DPNetTraffic*, demonstrou um desempenho significativamente superior. Foi observada uma redução média de pelo menos 35% no ruído introduzido aos dados.

Palavras-chave: privacidade de dados; privacidade diferencial; tráfego de redes; pós-processamento.

ABSTRACT

Network traffic data is extremely valuable and plays a fundamental role in a variety of applications. This information is collected by different entities, such as Internet service providers (ISPs), who often share or commercialize this data with external entities. However, sharing this data can potentially compromise the privacy of individuals whose information is contained within it. To address this privacy concern, we propose a new approach called *DPNetTraffic*. This approach utilizes the concept of differential privacy, which involves adding a controlled level of noise to the original data. This preserves the privacy of useful information in the data, as the shared data does not reveal specific and identifiable information about them. The *DPNetTraffic* approach stands out for its efficiency in preserving the privacy of useful information of network traffic data. Compared to other techniques that also adopt differential privacy, experimental results have shown that it introduces less noise to the data. This means that valuable insights and useful information can be obtained from the shared data while protecting the privacy of the individuals involved. The use of *DPNetTraffic* in sharing network traffic data represents a significant advancement in balancing data utility and user privacy protection. This approach has the potential to be adopted by entities that collect and share network traffic data, offering a reliable and effective solution to mitigate privacy breaches. In comparison to the specific baseline results, the proposed approach, named *DPNetTraffic*, demonstrated significantly superior performance. An average reduction of 35% in the introduced noise was observed in the data.

Keywords: data privacy; differential privacy; network traffic; post-processing.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

1.1 Motivação

Com a expansão de serviços e plataformas *web* na era digital, surge uma crescente demanda por coleta e monitoramento de dados de tráfego de redes (JOSHI; HADI, 2015). Esses dados são geralmente coletados, gerenciados e monitorados por provedores de serviço de *Internet* (*Internet Service Provider - ISP*), e se tornam essenciais para uma variedade de aplicações, tais como detecção de pontos de acessos, conhecimento do perfil de utilização da rede, identificação de comportamento anômalo de tráfego (segurança) e alocação adequada de recursos (SHAFIQ *et al.*, 2016).

Os provedores de serviço de internet têm uma importância essencial como empresas intermediárias na implementação de diversas atividades digitais, tais como serviços governamentais eletrônicos (e-Government), educação à distância (e-Learning), serviços bancários eletrônicos (e-Banking), negócios eletrônicos (e-Business) e entre outros (DHARMAWAN *et al.*, 2019). Por meio de suas redes de computadores, os provedores de serviço de internet concedem aos usuários finais acesso a diversas tecnologias baseadas em informação. Além disso, essas empresas são responsáveis por fornecer serviços de internet e informações eletrônicas para os usuários, ou seja, elas disponibilizam um portal para o ciberespaço, permitindo que os usuários acessem uma variedade de informações importantes e interessantes. (PARENTONI, 2009).

Uma atribuição crucial dos provedores de serviço de internet é gerenciar os dados de tráfego de rede, sendo primordial que realizem a coleta e análise dessas informações com eficiência e eficácia. Isso permite que eles forneçam serviços de alta qualidade aos seus clientes, além de garantir a segurança da rede (GARCÍA-DORADO *et al.*, 2012).

Dados de tráfego de rede são informações coletadas a partir do fluxo de dados que ocorre em uma rede de computadores por meio de várias fontes, como roteadores, switches, firewalls, proxies, computadores e entre outros dispositivos de rede. Esses dados incluem informações como endereços IP, tipo de protocolo utilizado, porta conectada, serviço acessado e outros metadados (TANENBAUM; WETHERALL, 2021).

Uma das aplicações mais relevantes dos dados de tráfego de rede é a detecção de pontos de acesso, sendo fundamental para a expansão de serviços de internet. Um ponto de acesso desempenha a função de receber e redistribuir um sinal de rede, seja ele transmitido por meio de uma conexão cabeada ou sem fio a outros dispositivos eletrônicos, tais como tablets,

smartphones, notebooks, smart TVs, entre outros. (KUROSE *et al.*, 2013). Com a ajuda desses dados, os provedores de serviço de internet podem identificar áreas carentes de conexão e trabalhar para melhorar a infraestrutura de rede nessas áreas (CASSOLA *et al.*, 2015).

Além disso, os dados de tráfego de rede também podem ser usados para entender melhor o perfil de uso da rede de computadores e identificar padrões de tráfego específicos. Com base nesses padrões, os provedores de serviços de internet podem adaptar seus serviços para atender às necessidades específicas de seus clientes e oferecer soluções personalizadas (STREIT *et al.*, 2019). Isso não só aumenta a satisfação do cliente, mas também pode ajudar a atrair novos clientes e a expandir a base de usuários.

Por fim, os dados de tráfego de rede são essenciais para garantir a segurança da rede e proteger contra possíveis ameaças cibernéticas. Com a ajuda desses dados, os provedores de serviços de internet podem identificar comportamentos anômalos de tráfego e tomar medidas para corrigi-los antes que eles causem danos à rede ou aos usuários (FURNO *et al.*, 2017).

Em suma, a coleta, o monitoramento e a análise de dados de tráfego de rede são fundamentais para o detecção de pontos de acessos, conhecimento do perfil de utilização da rede, identificação de comportamento anômalo de tráfego (segurança) e alocação adequada de recurso pelos provedores de serviço de internet. Com a análise eficaz desses dados, os provedores de serviço de internet podem oferecer serviços de alta qualidade, entender melhor as necessidades de seus clientes e garantir a segurança da rede contra possíveis ameaças cibernéticas.

No entanto, para que essas análises possam ser realizadas, os provedores de serviço de internet geralmente precisam compartilhar ou comercializar seus dados de tráfego de rede com entidades externas e tal fato pode levar a violações de privacidade dos indivíduos contidos nesses dados (MIRIMIR, 2018). Consequentemente, sanções podem ser aplicadas a essas empresas devido a falta de conformidade às leis de privacidade vigentes no país onde o dado é coletado (LGPD, 2019; GDPR, 2018; Comissão Federal de Comunicação, 2018).

Para garantir a proteção da privacidade dos usuários da Internet, diversas leis e regulamentos foram estabelecidos em diferentes países, como a Lei Geral de Proteção de Dados Pessoais no Brasil (LGPD, 2019), o Regulamento Geral de Proteção de Dados na Europa (GDPR, 2018), a Comissão Federal de Comunicação nos Estados Unidos (Comissão Federal de Comunicação, 2018) e muitos outros. Essas leis e regulamentos têm como objetivo estabelecer diretrizes para a coleta, uso e compartilhamento de dados pessoais, garantindo que os indivíduos tenham o controle sobre seus dados e que os provedores de serviço de internet estejam em

conformidade com as normas de privacidade e proteção de dados (WOLTERS, 2017).

A LGPD, em vigor desde 2020, estabelece regras claras para o tratamento de dados pessoais, impondo obrigações para as empresas que coletam e processam esses dados, além de garantir direitos aos titulares dos mesmos (LGPD, 2019). Já a GPDR, em vigor desde 2018, busca harmonizar as leis de privacidade de dados em toda a União Europeia, estabelecendo regras rígidas para a coleta e processamento desses dados (GDPR, 2018). A FCC, por sua vez, é uma agência reguladora dos Estados Unidos que tem como uma de suas principais funções a regulação das comunicações eletrônicas, incluindo a proteção de dados pessoais. A agência tem poder para impor multas e sanções às empresas que não seguem as regras de privacidade de dados estabelecidas (Comissão Federal de Comunicação, 2018).

Dessa forma, é crucial que os provedores de serviço de internet estejam cientes das leis e regulamentos de privacidade em seus respectivos países de atuação e implementem medidas eficazes para proteger os dados de seus usuários (WOLTERS, 2017).

Anonimizar os dados antes de compartilhá-los com terceiros é uma das estratégias mais promissoras para garantir a privacidade dos indivíduos (BRITO; MACHADO, 2017). Ao fazer isso, os dados deixam de ser considerados pessoais, tornando-se não aplicáveis às leis de privacidade vigentes (LGPD, 2019; GDPR, 2018; Comissão Federal de Comunicação, 2018).

Nesse contexto, várias técnicas de anonimização de dados foram propostas nas últimas décadas. O *K-anonimity* (SWEENEY, 2002) é um dos modelos de privacidade mais conhecidos que consistem em formar classes de registros de tamanho k. Em uma classe, cada registro é idêntico aos outros $(k-1)$ registros. Em outras palavras, cada registro não pode ser vinculado a um indivíduo com probabilidade inferior a $1/k$. A partir do *k-anonimity*, outros modelos de privacidade foram propostos para evitar a reidentificação de indivíduos em compartilhamento de dados, tais como *l-diversity* (MACHANAVAJJHALA *et al.*, 2007), δ*-presence* (NERGIZ *et al.*, 2007) e *t-closeness* (LI *et al.*, 2009).

Contudo, todas essas abordagens mencionadas pressupõem que um adversário (usuário malicioso) possui conhecimento limitado, o que não é verdadeiro em situações do mundo real. De fato, há diversas formas de ataques que podem ser realizados, como ataques de correlação e de inferência, que visam identificar indivíduos em um conjunto de dados anonimizados (SWEENEY, 2002; MACHANAVAJJHALA *et al.*, 2007). Para exemplificar, considere a contagem de serviços de *streaming* coletados por um ISP em uma determinada região do país, conforme Figura 1.

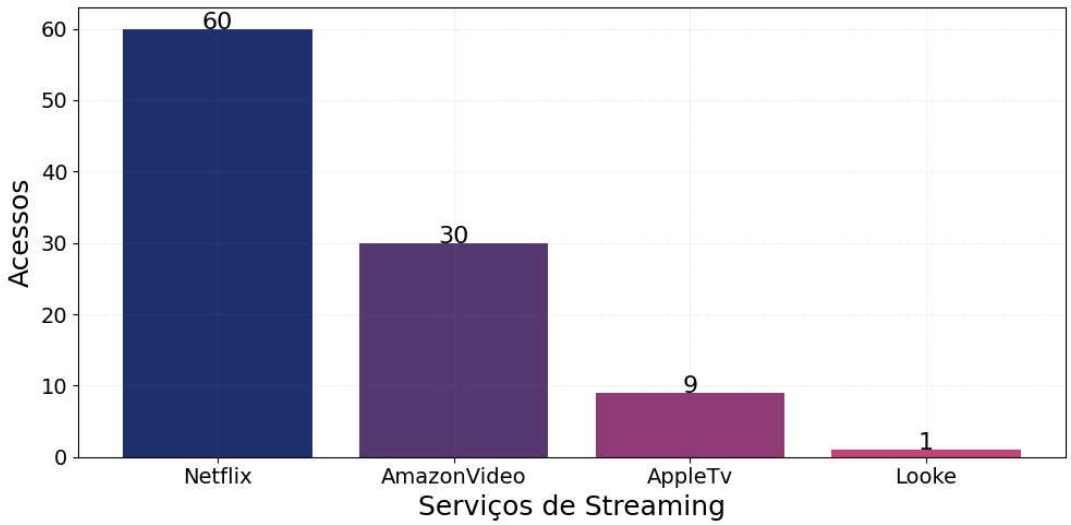


Figura 1 – Exemplo de dados de contagem de serviços de *streaming* coletados por um provedor de serviço de internet em uma determinada região do país.

No exemplo acima, tem-se um total de 100 usuários de serviços de *streaming*, dos quais 60 utilizam *Netflix*, 30 utilizam *AmazonVideo*, 9 utilizam *AppleTv* e apenas um indivíduo utiliza o serviço *Looke*. Considere que o provedor de serviço de internet, detentor desses dados, queira comercializá-los com a empresa *Looke*, a qual deseja descobrir quantos usuários estão utilizando seus serviços nessa região. Esse compartilhamento de dados pode ser útil para eventuais direcionamentos de marketing da empresa *Looke*, com o intuito de aumentar sua carteira de clientes na região. Caso o provedor de serviço de internet comercialize ou compartilhe os dados de tráfego da sua rede com a essa entidade externa, informações pessoais de seus clientes podem estar presentes no conjunto de dados compartilhado. Na Figura 1, caso um adversário, munido de informações externas, conheça o usuário que utiliza o serviço de *streaming Looke* na região, a privacidade deste usuário é violada, e assim, as leis de privacidade vigentes são descumpridas.

A Privacidade Diferencial (DWORK, 2006) é um modelo de privacidade que visa proteger a privacidade dos indivíduos enquanto permite que os dados sejam compartilhados e utilizados para fins de análise. Nos últimos anos, essa técnica tem se tornado o padrão para compartilhamento de dados de maneira privada (SANGEETHA; SADASIVAM, 2019). Ela consiste em adicionar um nível controlado de ruído aos dados originais de forma a impedir a identificação de indivíduos específicos no conjunto de dados compartilhado. Por meio desse modelo de privacidade, assume-se que um adversário possui conhecimento sobre $n-1$ registros do conjunto de dados, com exceção do registro sobre o qual estão tentando adquirir informações

(DWORK, 2006).

Logo, a Privacidade Diferencial assume que o conhecimento adversário sobre os dados é quase ilimitado. Essa suposição é feita para garantir que mesmo um adversário que possua acesso a várias fontes externas de informação não consiga utilizar essas informações para identificar indivíduos específicos nos dados compartilhados. Além disso, essa medida de segurança é aplicada mesmo que o adversário seja capaz de correlacionar diferentes conjuntos de dados, protegendo a privacidade dos indivíduos (DWORK, 2006).

É importante mencionar que, após a inserção de ruído, a utilidade dos dados para eventuais análises pode ser comprometida (DWORK *et al.*, 2006). Dessa forma, torna-se desafiador propor soluções que eficientemente adicionem ruído a dados de tráfego de rede de tal sorte que a privacidade dos indivíduos é protegida, enquanto a utilidade dos dados é mantida.

1.2 Problema Científico

Nesta dissertação nós investigamos o problema do compartilhamento privado de dados de tráfego de rede, os quais são coletados para obter informações sobre o uso da rede de computadores. Em particular, abordamos o problema do compartilhamento de três informações sobre tráfego de rede de maneira privada: contagem de portas, contagem de protocolos e contagem de serviços. Dessa forma, nossa pergunta de partida é: Como disponibilizar dados de tráfego de rede para que eventuais análises sejam realizadas sem revelar informações privadas do dado e, ao mesmo tempo, garantir que o resultado dessas análises sejam os mais próximos possíveis dos resultados originais?

1.3 Objetivos

1.3.1 Objetivos gerais

Tendo em vista o problema científico apresentado anteriormente, este trabalho propõe uma nova técnica para permitir aos provedores de serviços de internet e entidades que coletam dados de tráfego de rede compartilharem, ou comercializarem, seus dados por meio da privacidade diferencial, preservando a privacidade de informações do fluxo de rede, ao mesmo tempo em que busca manter a utilidade das informações extraídas dos dados privados.

1.3.2 Objetivos específicos

Em conformidade com o objetivo geral deste trabalho, foram estabelecidos os seguintes objetivos específicos:

1. Propor uma nova técnica, com base na Privacidade Diferencial, para permitir o compartilhamento ou comercialização de informações importantes sobre tráfego de rede, em particular contagem de portas, protocolos e serviços;
2. Agrupar os dados de tal sorte que a adição de ruído, via Privacidade Diferencial, seja executada apenas uma vez para cada contagem ao invés de três vezes seguindo a abordagem mais usual;
3. Obter as contagens agregadas, de maneira privada, por portas, protocolos e serviços ao mesmo tempo que garante que as contagens tenham valores positivos;
4. Uma abrangente análise sobre quatro conjuntos de dados reais para avaliar a acurácia da solução proposta quando comparada a outras técnicas que também adotam Privacidade Diferencial.

1.4 Produção Científica

O trabalho desta dissertação deu origem à seguinte publicação científica, na qual o *DPNetTraffic* é proposto. A publicação é apresentada a seguir:

1. MONTEIRO, Felipe C.; BRITO, Felipe T.; CHAVES, Iago C.; MACHADO, Javam C.. Compartilhamento de Dados de Tráfego de Rede Utilizando Privacidade Diferencial. In: SEMINÁRIO INTEGRADO DE SOFTWARE E HARDWARE (SEMISH), 50. , 2023.

1.5 Organização da Dissertação

O texto está organizado da seguinte maneira: No Capítulo 2, são apresentados os principais conceitos relacionados a Redes de Computadores, Tráfego de Redes e Privacidade Diferencial. No Capítulo 3, são descritos e discutidos trabalhos relevantes no contexto de privacidade de dados para tráfego de redes. Em seguida, no Capítulo 4, o *DPNetTraffic* e apresentado. Posteriormente, o Capítulo 5 apresenta a avaliação experimental, incluindo o ambiente de execução, as métricas utilizadas para mensurar a utilidade das respostas anonimizadas e os resultados obtidos. Por fim, o Capítulo 6 conclui o trabalho e sugere algumas possíveis direções de pesquisa para o futuro.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, apresentamos os conceitos fundamentais que estão diretamente relacionados a rede de computadores, ao tráfego de redes e à Privacidade Diferencial. Esses conceitos são essenciais para compreender a abordagem proposta neste trabalho e estabelecer uma base sólida para as discussões e análises realizadas.

2.1 Redes de Computadores e Tráfego de Redes

Redes de computadores é uma das áreas mais importantes e em constante evolução no campo da tecnologia da informação (TANENBAUM; WETHERALL, 2021). Uma rede de computadores é um conjunto de dispositivos interconectados, tais como computadores, impressoras, roteadores, switches e outros equipamentos, que podem se comunicar entre si para compartilhar recursos, dados e informações (KUROSE *et al.*, 2013).

Ela também é um dos pilares fundamentais da internet, permitindo a conexão e o tráfego de informações entre diferentes dispositivos em escala global (DHARMAWAN *et al.*, 2019). A rede de computadores é amplamente utilizada em empresas para compartilhar recursos, como impressoras e servidores, e permitir a comunicação entre departamentos e funcionários (TANENBAUM; WETHERALL, 2021). É graças a essa rede que podemos enviar e receber e-mails, mensagens instantâneas, fazer pesquisas, assistir a vídeos, entre outras atividades online (PARENTONI, 2009).

Segundo Peterson e Davie (2007), o tráfego de rede é um conceito importante no contexto de redes de computadores e, refere-se à transferência de informações entre diferentes dispositivos conectados em uma rede. Em uma rede de computadores, os dados são transmitidos em pacotes através dos diferentes dispositivos interconectados. Esses pacotes contêm informações sobre o destino da transmissão, a origem da transmissão, bem como os próprios dados que estão sendo transmitidos (KUROSE *et al.*, 2013).

Nesse contexto, as redes de computadores são organizadas em camadas, conforme descrito por Tanenbaum e Wetherall (2021). A transmissão de dados ocorre através de diferentes camadas que compõem o modelo de rede TCP/IP (Protocolo de Controle de Transmissão/Protocolo de Internet), um modelo de referência amplamente utilizado para comunicação em redes de computadores, que divide o processo de transmissão em quatro camadas (ALANI; ALANI, 2014).

Cada camada é responsável por diferentes aspectos do processo de comunicação, como a segmentação de dados em pacotes menores, a codificação e decodificação de informações, o estabelecimento de conexões e a transmissão e recebimento de pacotes de dados (KUROSE *et al.*, 2013). As camadas são uma forma de organizar a comunicação entre dispositivos em uma rede de computadores (ALANI; ALANI, 2014). Dessa forma, elas possibilitam uma abstração da complexidade da comunicação em rede, facilitando o desenvolvimento de protocolos e aplicativos que utilizam essa comunicação (TANENBAUM; WETHERALL, 2021).

A Camada de Aplicação é a camada mais alta e é responsável pela comunicação entre os processos de aplicação. É nessa camada que ocorre a interação entre o usuário final e o programa que está sendo utilizado (KUROSE *et al.*, 2013). A Camada de Transporte, logo abaixo da Camada de Aplicação, é encarregada por garantir que a informação seja entregue corretamente do remetente para o destinatário. Ela é responsável pelo controle de fluxo, pela verificação de erros e pela segmentação dos dados em pacotes menores para transmissão. A Camada de Rede tem a função de rotear os pacotes entre as diferentes redes de computadores. É responsabilidade da Camada de Rede encontrar o melhor caminho para que os pacotes possam chegar ao destino, independentemente do número de saltos que devem ser dados nos roteadores de origem até a chegada aos roteadores de destino (TANENBAUM; WETHERALL, 2021). Já a Camada de Acesso à Rede é responsável pela comunicação entre o dispositivo e a rede física. Ela é responsável pela transmissão dos pacotes entre o computador e os dispositivos de rede.

Como mencionado anteriormente, cada camada desempenha um papel específico na comunicação em rede de computadores e, juntas, garantem uma comunicação eficiente e confiável entre os dispositivos na internet (PETERSON; DAVIE, 2007; ALANI; ALANI, 2014). Embora as camadas possam parecer complexas, elas são essenciais para garantir que os dados sejam transmitidos com segurança, confiabilidade e eficiência através da rede de computadores.

Os provedores de serviço de internet (ISP – Internet Service Provider) desempenham um papel crucial no tráfego de dados em redes de computadores, pois são responsáveis por gerenciar e direcionar o tráfego de dados através de suas redes de computadores (DHARMAWAN *et al.*, 2019). Eles são os responsáveis por garantir que os pacotes de dados sejam roteados para seus destinos corretos, evitando congestionamento e interrupções no fluxo de rede (KUROSE *et al.*, 2013; TANENBAUM; WETHERALL, 2021).

Eles também são responsáveis por fornecer o acesso à internet, bem como pela manutenção da infraestrutura de rede necessária para que seus clientes se conectem (DHARMAWAN

et al., 2019). Em outras palavras, os provedores de serviço de internet são os intermediários entre os usuários finais e a internet, oferecendo uma vasta gama de serviços e informações online.

Um exemplo de tráfego de rede pode ser visto na Figura 2: o usuário final envia uma solicitação de acesso a um site por meio de um navegador da web. Este, por sua vez, envia a solicitação para o provedor de serviços de internet (ISP), que encaminha a solicitação para o servidor que hospeda o site/serviço solicitado. O servidor processa a solicitação e envia a resposta de volta para o usuário, seguindo o mesmo caminho, mas em sentido inverso. Esse é um exemplo de como o tráfego de rede é gerado, mostrando como os dados são transmitidos pela rede de computadores do provedor de serviço de internet para acessar informações online.

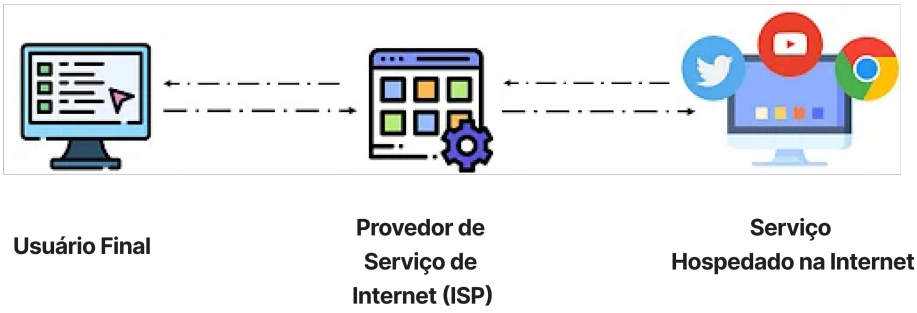


Figura 2 – Exemplo de como os dados são transmitidos pela rede de computadores para acessar informações online.

Para realizar tal tarefa, os provedores de serviço de internet utilizam identificadores únicos gerenciados pela IANA (Internet Assigned Numbers Authority), como endereços IP, números de porta e protocolos (WEIL *et al.*, 2012).

A IANA é uma organização responsável pela atribuição de identificadores padronizados para a Internet, como endereços IPs, números de portas, protocolos e outros parâmetros (IANA, 2023). Os endereços IPs permitem aos provedores de serviço de internet rotear o tráfego de rede entre os dispositivos conectados à sua rede, enquanto as portas são usadas para direcionar o tráfego para os serviços corretos em seus servidores e os protocolos definem como os dados são formatados, transmitidos e recebidos (TANENBAUM; WETHERALL, 2021).

2.2 Conjunto de Dados de Tráfego de Redes

Um conjunto de dados de tráfego de redes consiste em diversos registros de informações sobre o tráfego de dados em uma rede de computadores (KUROSE *et al.*, 2013). Esses registros incluem informações como o endereços IPs dos pacotes de dados, portas e protocolos utilizados, os serviços acessados, a quantidade de dados transferidos e entre outras métricas (TANENBAUM; WETHERALL, 2021).

Um conjunto de dados de tráfego de redes é uma fonte valiosa de informações para diversos propósitos, tais como análise de desempenho, segurança e diagnóstico de problemas na rede. Por exemplo, pode ser possível identificar gargalos de tráfego em determinados horários, detectar possíveis ataques de rede ou avaliar a eficácia de medidas de segurança implementadas (TANENBAUM; WETHERALL, 2021).

Um exemplo de um conjunto de dados de tráfego de rede utilizado neste trabalho pode ser visto na Tabela 1. A coluna *IP Destino* abrange os endereços IPs de destino dos fluxos de rede, a coluna *Porta Destino* refere-se às portas utilizadas no fluxo, já a coluna *Protocolo* indica o tipo de protocolo utilizado na comunicação e a coluna *Serviço* contêm os nomes das aplicações dos fluxos de rede.

IP Destino	**Porta Destino**	**Protocolo**	**Serviço**
13.32.84.48	80	TCP	AmazonVideo
45.57.41.1	443	TCP	Netflix
23.32.65.164	445	TCP	AppleTV
17.249.156.80	443	UDP	Youtube
173.194.55.105	443	UDP	Youtube
35.164.74.30	53	TCP	Netflix
54.192.57.252	80	TCP	AmazonVideo
10.200.7.7	80	TCP	AmazonVideo
35.164.118.134	443	TCP	Netflix
17.42.254.14	445	TCP	AppleTV
179.1.4.206	443	UDP	Youtube
172.16.255.200	53	TCP	Netflix
74.125.134.127	53	UDP	Looke
	...		

Tabela 1 – Exemplo de um conjunto dados de tráfego de rede.

A análise do tráfego de redes de computadores é o processo de examinar o tráfego de dados em uma rede de computadores para obter informações sobre o comportamento da

rede, identificar problemas de desempenho, falhas de segurança e outras questões relacionadas à rede (TANENBAUM; WETHERALL, 2021). Os dados de rede são geralmente coletados por ferramentas de análise de tráfego de rede, que podem capturar e examinar dados em tempo real ou a partir de logs armazenados.

O Wireshark[1], o tcpdump[2] e ntop[3] são exemplos de ferramentas que permitem a visualização dos dados coletados, a análise de padrões e tendências, além de possibilitar a identificação de problemas na rede (HINTZE *et al.*, 2022). Os autores em Ndatinya *et al.* (2015) apresentam alguns casos práticos de como essas ferramentas podem ser aplicadas na análise do tráfego de redes. Isso inclui a identificação de padrões de tráfego suspeitos, detecção de atividades maliciosas, reconstrução de sessões de comunicação, análise de conteúdo de pacotes, entre outros aspectos relevantes para investigações do tráfego de redes.

No entanto, é importante salientar que a coleta e análise desses dados podem representar uma ameaça à privacidade, uma vez que informações privadas dos dados podem ser expostas (BREWSTER, 2017). A Privacidade Diferencial surge como uma resposta para essa questão, oferecendo uma solução que permite o compartilhamento e a análise segura dos dados, ao mesmo tempo em que preserva a privacidade dos usuários.

2.3 Privacidade Diferencial

Privacidade Diferencial é um conceito importante em ciência de dados que visa proteger a privacidade das informações pessoais dos indivíduos, permitindo que as informações sejam utilizadas para análise estatística sem expor dados individuais (DWORK *et al.*, 2014). Nos últimos anos, essa técnica tem se tornado o padrão para compartilhamento de dados de maneira privada (SANGEETHA; SADASIVAM, 2019). Isso é especialmente importante em situações em que dados confidenciais são coletados, como em pesquisas médicas, censo populacional ou até mesmo em empresas que coletam dados de seus clientes, como por exemplo os provedores de serviço de internet (ISP).

As violações de privacidade ocorrem por meio de ataques nos quais um adversário é capaz de vincular a identidade de um indivíduo a um registro em um conjunto de dados, utilizando informações previamente obtidas de uma fonte externa. Por exemplo, o adversário pode saber que a vítima reside ao lado de sua própria residência, permitindo inferir informações

[1] https://www.wireshark.org/
[2] https://www.tcpdump.org/
[3] https://www.ntop.org/

como endereço, CEP, sexo, entre outros dados sensíveis. Essas associações de dados podem comprometer a privacidade e revelar informações pessoais sem o consentimento do indivíduo afetado (BRITO; MACHADO, 2017). A Privacidade Diferencial dificulta a reidentificação de indivíduos a partir de ataques de ligação, em que o atacante possui um conhecimento prévio por meio de fontes externas (DWORK *et al.*, 2014). Isso é feito adicionando ruído estatístico aos dados, de modo que as informações que possam ser reveladas pelo conjunto de dados original sejam anonimizadas (DWORK, 2006).

A Privacidade Diferencial permite que pesquisadores e analistas acessem informações úteis do conjunto de dados, sem que essas informações possam ser usadas para identificar um indivíduo específico. Além disso, ela garante a privacidade contra ataques de adversários mal-intencionados, que tentam descobrir informações pessoais a partir do conjunto de dados disponível (DWORK *et al.*, 2006).

Na Figura 3 é possível visualizar o fluxo de funcionamento da Privacidade Diferencial.

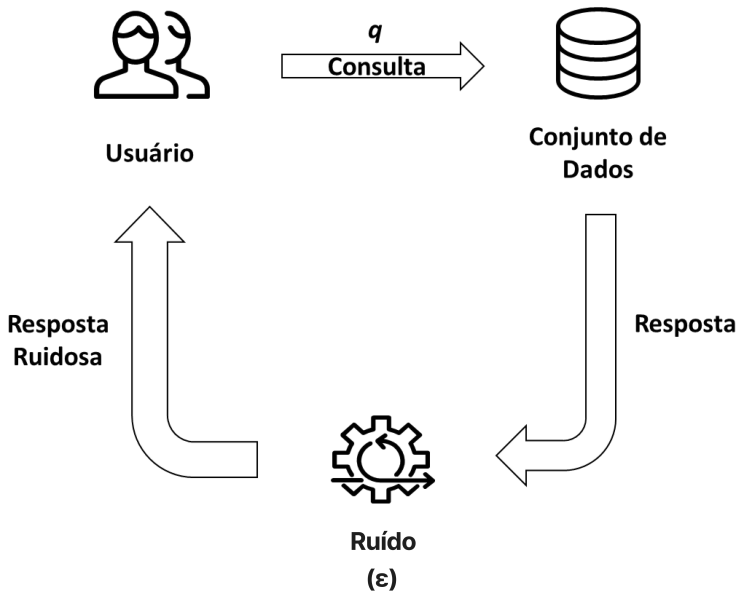


Figura 3 – Fluxo de funcionamento da Privacidade Diferencial.

No contexto da Privacidade Diferencial, um atacante é uma entidade que tem acesso a um conjunto de dados sobre indivíduos e que deseja obter informações sobre um determinado indivíduo representado ou não no conjunto de dados (DWORK *et al.*, 2014). Essa entidade pode ser mal-intencionada e tentar usar as informações para fins ilegais, como roubo de identidade ou

fraude, ou pode ser uma empresa que deseja usar as informações para segmentar o mercado ou melhorar seus produtos e serviços (YANG *et al.*, 2012).

Um atacante pode ter diferentes níveis de conhecimento sobre os dados e diferentes recursos para tentar obter informações (DWORK *et al.*, 2006). Por exemplo, um atacante pode ter acesso apenas a uma pequena parte dos dados, enquanto outro pode ter acesso a todo o conjunto de dados. Da mesma forma, um atacante pode ter recursos limitados para realizar ataques, enquanto outro pode ter recursos ilimitados para tal (BRITO; MACHADO, 2017).

O objetivo do uso de técnicas como a Privacidade Diferencial é proteger os dados dos ataques desses diferentes tipos de atacantes, garantindo que os dados permaneçam privados e seguros, mesmo quando há tentativas de obter informações sobre eles (DWORK *et al.*, 2014).

2.3.1 Definição Formal

A Privacidade Diferencial é satisfeita por um algoritmo aleatório, geralmente chamado de *mecanismo* $\mathscr{M}$, capaz de adicionar um ruído apropriado para gerar uma resposta à uma consulta realizada pelo usuário. Esse mecanismo é controlado por um parâmetro denominado *orçamento de privacidade* ε (ou do inglês - *privacy budget*) (DWORK, 2006). Um valor pequeno de ε corresponde diretamente a uma maior garantia da preservação de privacidade, ou seja, uma maior quantidade de ruído adicionado ao dado original.

Em geral, para se definir um orçamento de privacidade adequado para uma aplicação, especialistas devem realizar um amplo estudo para garantir que a privacidade dos indivíduos seja suficientemente protegida, mantendo bons níveis de precisão nas informações compartilhadas, isto é, uma boa utilidade dos dados (BUREAU, 2021).

Já o trabalho da Dwork *et al.* (2019), propõe que empresas sejam incentivadas a fornecer informações sobre suas implementações de Privacidade Diferencial através da adoção de um *"Registro de Orçamento de Privacidade"* que utiliza o parâmetro ε. Esse *Registro* tem como objetivo apoiar o compartilhamento de conhecimento, permitindo que as organizações aprendam com as escolhas feitas por outras. Além disso, o *Registro* atua como um mecanismo de supervisão, oferecendo transparência em relação às práticas e escolhas adotadas pelas instituições que coletam e compartilham dados atendendo privacidade diferencial (DWORK *et al.*, 2019).

Neste trabalho, utilizamos uma variação do orçamento de privacidade de $0,1$ a $1,0$ (Capitulo 4), valores comumente reportados na literatura, independente da aplicação.

Formalmente, a privacidade diferencial é definida por:

Definição 1 *(Privacidade Diferencial (DWORK, 2006)) Um mecanismo aleatório $\mathscr{M}$ satisfaz Privacidade Diferencial, se para todos os conjuntos de dados vizinhos $\mathscr{D}_1$ e $\mathscr{D}_2$ que diferem em pelo menos um elemento e para qualquer possibilidade de saída O de $\mathscr{M}$,*

$$Pr[\mathscr{M}(\mathscr{D}_1) = O] \leq exp(\varepsilon)Pr[\mathscr{M}(\mathscr{D}_2) = O],$$

onde Pr[·] indica a probabilidade de um dado evento.

2.3.2 Conjunto de Dados Vizinhos

A Privacidade Diferencial protege a privacidade dos indivíduos baseada no conceito de indistinguibilidade de conjunto de dados. Considere uma função de consulta de contagem $q : \mathscr{D} \rightarrow \mathbb{Z}$ onde $\mathscr{D}$ indica o conjunto de possibilidades de todos os conjuntos de dados. A função de consulta de contagem q é aplicada em um conjunto de dados e retorna um número inteiro. A Privacidade Diferencial se baseia no conceito de conjunto de dados vizinhos. Dois conjuntos de dados $\mathscr{D}_1 \in \mathscr{D}$ e $\mathscr{D}_2 \in \mathscr{D}$ são ditos *conjuntos de dados vizinhos* se eles diferem em um registro, isto é, $|\mathscr{D}_1 - \mathscr{D}_2| = 1$ (DWORK, 2006).

Para exemplificar o conceito de conjunto de dados vizinhos, considere o conjunto de dados $\mathscr{D}$ na Figura 4a. Uma das possibilidades de seus vizinhos pode ser obtido pela remoção de seu último registro, resultando na Figura 4b, uma vez que a remoção de seu último registro não altera os valores dos demais registros.

IP Dest.	Porta Dest.	Protocolo	Serviço
13.32.84.48	80	TCP	AmazonVideo
45.57.41.1	443	TCP	Netflix
23.32.65.164	445	TCP	AppleTV
17.249.156.80	443	UDP	Youtube
173.194.55.105	443	UDP	Youtube
35.164.74.30	53	TCP	Netflix
54.192.57.252	80	TCP	AmazonVideo

(a)

IP Dest.	Porta Dest.	Protocolo	Serviço
13.32.84.48	80	TCP	AmazonVideo
45.57.41.1	443	TCP	Netflix
23.32.65.164	445	TCP	AppleTV
17.249.156.80	443	UDP	Youtube
173.194.55.105	443	UDP	Youtube
35.164.74.30	53	TCP	Netflix

(b)

Figura 4 – Exemplo de conjunto de dados vizinhos de tráfego de rede.

Existem diversas técnicas que podem ser utilizadas para atender à Privacidade Diferencial (DWORK, 2008), que tem como objetivo assegurar que os resultados produzidos por um mecanismo não permitam distinguir, por meios computacionais, conjuntos de dados

vizinhos, ou seja, que diferem em, no máximo, um indivíduo. Uma das formas mais comuns de garantir privacidade diferencial é através da adição de ruído às respostas de consultas, como exemplificado na Figura 3 (DWORK, 2006).

2.3.3 Sensibilidade

Como mencionado anteriormente, a Privacidade Diferencial é atendida através de um mecanismo $\mathscr{M}$, que atua adicionando uma certa quantidade de ruído aleatório às respostas das consultas. O ruído adicionado, além de ser dependente do *orçamento de privacidade* ε, é também dependente da sensibilidade global da consulta realizada.

Formalmente, a sensibilidade Global é definida por:

Definição 2 *(Sensibilidade Global) A sensibilidade Global de uma consulta q é definida por:*

$$\Delta q = \max_{\mathscr{D}_1, \mathscr{D}_2} \| q(\mathscr{D}_1) - q(\mathscr{D}_2) \|_1$$

, para todo $\mathscr{D}_1 \in \mathscr{D}$ *e* $\mathscr{D}_2 \in \mathscr{D}$ *(DWORK, 2006).*

A sensibilidade Global mede o maior impacto em relação à presença ou ausência de um registro em todos os possíveis pares de conjuntos de dados vizinhos. Quando q é uma consulta (função) de contagem, a sensibilidade Global $\Delta q = 1$, uma vez que a adição ou remoção de qualquer registro em um conjunto de dados pertencente a $\mathscr{D}$ impacta em no máximo 1 sobre qualquer consulta de contagem.

A sensibilidade de uma consulta é um parâmetro importante na Privacidade Diferencial, pois determina a quantidade de ruído estatístico que deve ser adicionada aos dados para preservar a privacidade (DWORK *et al.*, 2006). Quanto maior o valor de Δ, maior será a sensibilidade e, consequentemente, maior será a quantidade de ruído necessária para mascarar a remoção de um indivíduo. Portanto, é fundamental calcular corretamente a sensibilidade para garantir que a privacidade dos dados seja mantida (NEAR; ABUAH, 2021).

2.3.4 Propriedades

Além de sua capacidade de preservar a privacidade individual, a Privacidade Diferencial também apresenta algumas propriedades úteis, tais como o pós-processamento, a composição sequencial e composição paralela.

Definição 3 *(Pós-Processamento) Considere $\mathscr{M}$ qualquer mecanismo aleatório tal qual $\mathscr{M}(q)$ é diferencialmente privado. Para qualquer função f, $f(\mathscr{M}(q))$ também satisfaz Privacidade Diferencial (DWORK, 2006).*

A propriedade de Pós-Processamento define que qualquer função aplicada sobre uma saída de um mecanismo diferencialmente privado também satisfaz à Privacidade Diferencial (DWORK, 2006). Em outras palavras, se um mecanismo $\mathscr{M}$ for diferencialmente privado, então qualquer função aplicada ao resultado produzido por $\mathscr{M}$ também será diferencialmente privada. Isso significa que o resultado do mecanismo $\mathscr{M}$ pode ser usado como entrada para outras análises e ainda manter a garantia de privacidade.

Por exemplo, suponha que uma empresa de segurança de redes colete informações de tráfego de rede de seus usuários, incluindo informações como endereço IP, porta, protocolo e serviço. Seu objetivo é fornecer conclusões sobre o tráfego de rede para seus clientes, mas eles precisam garantir a privacidade dos usuários. Para proteger a privacidade dos usuários, a empresa decide usar a Privacidade Diferencial. Eles aplicam um mecanismo $\mathscr{M}$ de Privacidade Diferencial aos dados de tráfego de rede coletados, que adiciona ruído estatístico aos dados. Então, eles usam a média dos dados para calcular o tráfego médio de rede para um determinado serviço. O resultado final será uma aproximação do tráfego médio de rede, que é protegido pela Privacidade Diferencial. Isso significa que, mesmo que um atacante tenha acesso aos dados do conjunto de dados original, não será possível descobrir informações sobre um usuário específico. Além disso, a empresa pode aplicar outras funções estatísticas aos dados, como desvio padrão ou percentis, sem comprometer a privacidade dos usuários.

Definição 4 *(Composição Sequencial) Para cada mecanismo $\mathscr{M}_i$ que provê ε_i-privacidade diferencial, uma sequência de mecanismos diferencialmente privados $\mathscr{M}_i$, provê $\sum_i \varepsilon_i$-privacidade diferencial (MCSHERRY, 2009).*

Já a Composição Sequencial é aplicada quando executamos uma série de mecanismos sequencialmente no mesmo conjunto de dados. Isto é, algorítimos que realizam consultas nos dados mais de uma vez (NEAR; ABUAH, 2021). Isso implica que o orçamento de privacidade ε usado em cada consulta sobre o mesmo conjunto de dados precisa ser dividido (MCSHERRY, 2009).

Para ilustrar essa propriedade, suponha que uma empresa deseje compartilhar informações de tráfego de rede para fins de pesquisa, mas precisa garantir a privacidade dos usuários.

Eles podem aplicar um mecanismo de Privacidade Diferencial para adicionar ruído estatístico aos dados, de modo que as informações pessoais não possam ser identificadas. No entanto, o mecanismo adiciona um certo nível de ruído, o que pode afetar a utilidade dos dados para fins de análise. Para equilibrar a privacidade e a utilidade, a empresa pode dividir seu orçamento de privacidade para diferentes consultas de pesquisa. Por exemplo, eles podem optar por usar menos ruído em uma consulta mais importante, mas aplicar mais ruído em outras consultas menos críticas. Isso permite que a empresa maximize a utilidade dos dados, enquanto ainda protege a privacidade dos usuários.

Definição 5 *(Composição Paralela) Seja* $\mathscr{M}_i : \mathscr{D}^n \to \mathbb{Z}$ *um algorítimo que provê* ε_i*-privacidade diferencial para* $i \in [k]$ *e sejam* $x_1, ..., x_k$ *subconjuntos mutuamente disjuntos de* $\mathscr{D}^n$*. Então,* $M(x) = (M_1(x_1), \ldots, M_k(x_k))$ *é* $(\max_i \varepsilon_i)$*-diferencialmente privado (PATIL; SINGH, 2014).*

A Composição Paralela se aplica quando as consultas são realizadas em subconjuntos disjuntos de um conjunto de dados. Essa propriedade se baseia no princípio de que, ao dividir os dados em partes disjuntas, é possível realizar cálculos estatísticos ou análises sem comprometer a privacidade dos indivíduos. Cada parte contém uma porção específica dos dados, garantindo que as informações sensíveis permaneçam segregadas e protegidas (NEAR; ABUAH, 2021).

Para exemplificar essa propriedade, suponha que temos um conjunto de dados de tráfego de redes que contém informações sobre as portas de destino, os protocolos e serviços utilizados. Queremos obter a contagem para cada combinação única de portas de destino, protocolos e serviços. Para preservar a privacidade dos usuários, aplicamos a Privacidade Diferencial a essa análise. Em vez de calcular a contagem diretamente sobre o conjunto de dados original, dividimos o conjunto de dados em partes disjuntas, cada uma contendo um subconjunto de informações, por exemplo, através do agrupamento destes dados.

Em seguida, aplicamos um mecanismo de Privacidade Diferencial, como a adição de ruído aleatório, a cada parte para calcular as contagens das combinações únicas. Como as partes são disjuntas, a privacidade dos indivíduos é preservada, pois seus dados estão distribuídos entre as diferentes partes. Segundo Farias *et al.* (2023), o custo de privacidade para esse cenário é menor quando comparado com a Composição Sequencial, pois minimiza a exposição dos dados sensíveis durante o processamento.

2.3.5 Mecanismos

Como discutido anteriormente, a Privacidade Diferencial é atendida por um algoritmo aleatório, comumente chamado de *mecanismo* $\mathscr{M}$ (DWORK *et al.*, 2006). Os mecanismos em Privacidade Diferencial são ferramentas utilizadas para proteger a privacidade dos indivíduos em conjuntos de dados, permitindo que sejam realizadas análises estatísticas e inferências sem comprometer a identidade dos indivíduos presentes no conjunto de dados. Diferentes tipos de mecanismos são utilizados na Privacidade Diferencial, cada um com suas próprias características e métodos de aplicação. Nesta seção, discutem-se os mecanismos utilizados neste trabalho.

2.3.5.1 Mecanismo Laplace

Um dos *mecanismos* $\mathscr{M}$ mais comuns e simples para alcançar a Privacidade Diferencial é o Mecanismo de Laplace (DWORK, 2006). Esse mecanismo consiste na adição de ruído, utilizando uma variável aleatória da distribuição de Laplace. Dessa forma, a probabilidade de que uma consulta resulte em um determinado valor é influenciada pelo ruído adicionado, garantindo que a privacidade dos indivíduos no conjunto de dados seja preservada.

Teorema 1 *(Mecanismo Laplace (DWORK, 2006)) Dada uma consulta* $q : \mathscr{D} \to \mathbb{R}$*, o mecanismo Laplace* $\mathscr{M}$*:*

$$\mathscr{M}_q(\mathscr{D}) = q(\mathscr{D}) + Laplace(0, \tfrac{\Delta q}{\varepsilon})$$

fornece ε*-Privacidade Diferencial. Onde* $Laplace(0, \frac{\Delta q}{\varepsilon})$ *retorna uma variável aleatória da distribuição de Laplace com média zero e escala* $\frac{\Delta q}{\varepsilon}$*.*

2.3.5.2 Mecanismo Geométrico

Um outro mecanismo $\mathscr{M}$ utilizado é o Mecanismo Geométrico (GHOSH *et al.*, 2009), uma variante discreta do mecanismo de Laplace, que é usualmente adotado para consultas com respostas inteiras, no caso deste trabalho, consultas de contagem. A distribuição geométrica simétrica, com média 0 e parâmetro $\alpha \in [0, 1]$, é a distribuição de probabilidade tal que, para todos os inteiros x, uma variável aleatória X tem função de massa de probabilidade:

Teorema 2 *(Mecanismo Geométrico (GHOSH et al., 2009)) Dada uma consulta* $q : \mathscr{D} \to \mathbb{Z}$ *onde* $\mathscr{D}$*:*

$$Pr[X = x] = \tfrac{1-\alpha}{1+\alpha}\alpha^{|x|}$$

O mecanismo geométrico $\mathscr{M}$ que adiciona ruído independente a partir da distribuição geométrica simétrica, com $\alpha = exp(-\varepsilon/\Delta q)$, satisfaz Privacidade Diferencial.

Assim como o Mecanismo de Laplace (DWORK, 2006), o Mecanismo Geométrico (GHOSH *et al.*, 2009) possui um orçamento de privacidade ε, que controla a quantidade de ruído adicionado. Isso é, quanto maior o valor do orçamento de privacidade ε, menor será o ruído adicionado, mas menor será a privacidade garantida.

2.3.5.3 Mecanismo Log-Laplace

O Mecanismo de Log-Laplace também é outra técnica comum utilizada para satisfazer à Privacidade Diferencial em análise de dados sensíveis (NY; PAPPAS, 2013). Ele funciona adicionando ruído aleatório à resposta de uma consulta, como o mecanismo de Laplace, mas com uma distribuição de Laplace logarítmica. Ele é especialmente útil para valores extremos ou raros que aparecem com baixa frequência em uma distribuição de dados (NY; PAPPAS, 2013).

Teorema 3 *(Mecanismo Log-Laplace (NY; PAPPAS, 2013)) Dada uma consulta $q : D \to \mathbb{R}^k$ k-dimensional em uma base de dados $\mathscr{D}$, e $\varepsilon > 0$ um parâmetro de privacidade:*

$G(s) - \widehat{G}(s) = \frac{1}{s+1}\frac{\sum_{i=1}^{n}\mu_i}{n}$,

Então, o mecanismo $M : D \to \mathbb{R}^k$ dado por $M(d) = q(d) + \mathbf{X}$, onde $\mathbf{X} = (X_1, ..., X_k)$ e X_i é amostrado da distribuição Log-Laplace com parâmetro de escala $\frac{\Delta q}{\varepsilon}$, satisfaz ε-diferencial privacidade.

O Mescanismo Log-Laplace $\mathscr{M}$ adiciona um peso extra na cauda da distribuição Laplace para preservar ainda mais a privacidade dos dados e ao adicionar esse peso extra, a probabilidade de valores extremos (ou valores anômalos) é reduzida (NY; PAPPAS, 2013).

2.3.5.4 Dados Sintéticos

Uma outra alternativa para atender à Privacidade Diferencial, em vez de adicionar ruído às respostas originais, é utilizar a geração de dados sintéticos. Um conjunto de dados sintéticos é uma versão substituta de um conjunto de dados original que possui o mesmo formato e reflete fielmente as propriedades estatísticas do conjunto de dados original, mas contém apenas registros fictícios ou falsos (ULLMAN, 2022).

Os autores em Abowd *et al.* (2021), afirmam que de maneira intuitiva, podemos utilizar um conjunto de dados sintéticos da mesma forma que utilizaríamos o conjunto de dados reais. Assim podemos fazer análise sobre o conjunto de dados, calcular estatísticas resumidas e treinar modelos de inteligência artificial. A diferença é que, como os registros não correspondem a pessoas "reais", não há necessidade de nos preocuparmos em proteger a privacidade (ABOWD *et al.*, 2021).

Ganev *et al.* (2022) mencionam que os três mais populares geradores de dados sintéticos que satisfazem à Privacidade Diferencial são: o Privbayes (ZHANG *et al.*, 2017) – baseado em redes Bayesianas estatísticas e dois GANs (Generative Adversarial Networks) – O DP-WGAN (CRESWELL *et al.*, 2018) e o PATE-GAN (JORDON *et al.*, 2019), que incorporam mecanismos de Privacidade Diferencial.

É importante mencionar que diferentes modelos generativos de dados sintéticos que satisfazem à Privacidade Diferencial se comportam de maneira distinta (GANEV *et al.*, 2022). Por exemplo, PATE-GAN tem um desempenho melhor do que DP-WGAN, enquanto o PrivBayes é o único que consegue manter a utilidade dos dados em conjuntos de dados com diferentes tipos de atributos, isto é, contendo atributos com dados numéricos, categóricos e booleanos.

Para fins de referência, o Privbayes é o modelo adotado neste estudo para a geração de dados sintéticos. Essa escolha baseia-se no fato de que os conjuntos de dados utilizados apresentam uma variedade de atributos de diferentes tipos.

O PrivBayes utiliza redes Bayesianas para modelar as relações entre as variáveis nos dados. Em seguida, o algoritmo usa uma série de técnicas para preservar a privacidade dos dados, incluindo perturbação de parâmetros, amostragem e arredondamento. Essas técnicas garantem que os dados sintéticos gerados pelo algoritmo não possam ser rastreados de volta aos dados originais, mantendo assim a privacidade dos indivíduos presentes nos dados (ZHANG *et al.*, 2017).

Além disso, o PrivBayes foi projetado para ser escalável e eficiente em termos computacionais. Ele pode ser aplicado em grandes conjuntos de dados com muitas variáveis e pode gerar dados sintéticos com a mesma distribuição das variáveis originais, garantindo que os resultados finais sejam precisos e úteis para análise estatística. Neste contexto, o PrivBayes é considerado mais adequado neste trabalho, pois é capaz de lidar efetivamente com a diversidade de atributos e preservar as características estatísticas essenciais dos dados originais.

2.4 Conclusão

Neste capítulo foram apresentados os principais conceitos relacionados a Redes de Computadores, Tráfego de Dados, Privacidade Diferencial, suas propriedades e seus Mecanismos $\mathscr{M}$. Redes de computadores geram grandes quantidades de dados de tráfego, muitas vezes contendo informações sensíveis e confidenciais de seus usuários. Para proteger a privacidade dos usuários contidos nestes dados, é importante aplicar técnicas de Privacidade Diferencial que garantem que informações confidenciais não sejam reveladas durante a análise dos mesmos. Além disso, é importante lembrar que a aplicação dos mecanismos pode afetar a precisão dos resultados obtidos a partir da análise dos dados, o que deve ser levado em consideração na escolha do mecanismo.

3 TRABALHOS RELACIONADOS

Este capítulo apresenta alguns trabalhos relevantes para a área de privacidade de dados, que focam no contexto específico de tráfego de redes. As soluções de privacidade apresentadas a seguir consistem, em sua maioria, em análises do tráfego de rede e aplicações do conceito de Privacidade Diferencial. Ao examinar os trabalhos relacionados, é possível observar uma variedade de desafios abordados, soluções propostas e avaliações realizadas para avaliar a privacidade e utilidade dos dados de tráfego de redes. A análise desses trabalhos oferece uma compreensão mais aprofundada das abordagens existentes e suas contribuições para a preservação da privacidade de dados nesse contexto específico.

3.1 Vuvuzela: Scalable Private Messaging Resistant to Traffic Analysis

O trabalho apresentado por Hooff *et al.* (2015), é um estudo que propõe um novo sistema de mensagens privadas escalável, capaz de resistir à análise de tráfego de rede com base na Privacidade Diferencial. O problema abordado no trabalho é a dificuldade de implementar mensagens privadas pela Internet, uma vez que, mesmo que os dados das mensagens estejam criptografados, é desafiador ocultar os metadados que revelam informações sobre as partes envolvidas na comunicação.

Sistemas existentes oferecem garantias de privacidade, como o Dissent[1], mas são limitados em escala, suportando apenas alguns milhares de clientes. Por outro lado, sistemas escaláveis, como o Tor[2], não protegem contra a análise de tráfego de rede, tornando-os ineficazes em um contexto de monitoramento de rede generalizado.

O Vuvuzela é apresentado como uma solução escalável que oferece garantias sólidas de privacidade, ocultando tanto os dados das mensagens quanto os metadados. O sistema é projetado para resistir a adversários que observam e manipulam todo o tráfego de rede e controlam todos os nós, exceto um servidor. O Vuvuzela utiliza uma abordagem que minimiza as variáveis observáveis por um atacante e incorpora técnicas de Privacidade Diferencial para adicionar ruído às variáveis observáveis, garantindo que as informações sobre quais usuários estão se comunicando sejam ocultadas de forma comprovada.

Para compreender melhor por que a privacidade é difícil de ser garantida no modelo adversarial robusto do Vuvuzela, os autores consideraram um sistema com apenas um servidor, no

[1] https://dedis.cs.yale.edu/dissent/
[2] https://www.torproject.org/

qual o servidor é totalmente confiável. Mesmo nesse sistema, alcançar a privacidade não é trivial. Suponha que o servidor opere em rodadas fixas, coletando primeiro as mensagens de todos os clientes que desejam enviar uma mensagem e, em seguida, enviando cada mensagem para o seu destinatário. Embora o adversário não possa identificar imediatamente o remetente responsável por uma determinada mensagem do destinatário, ele ainda pode descobrir informações relevantes. Por exemplo, se o adversário suspeitar que Alice e Bob estão se comunicando, ele pode bloquear temporariamente o tráfego de rede de Alice e verificar se Bob deixa de receber mensagens. Ou, em nosso modelo de adversário forte, ele pode bloquear o tráfego de todos os clientes, exceto Alice e Bob, e verificar se alguma mensagem foi trocada quando apenas eles estão online. Um exemplo de como este fluxo é operado pode ser visto na Figura 5.

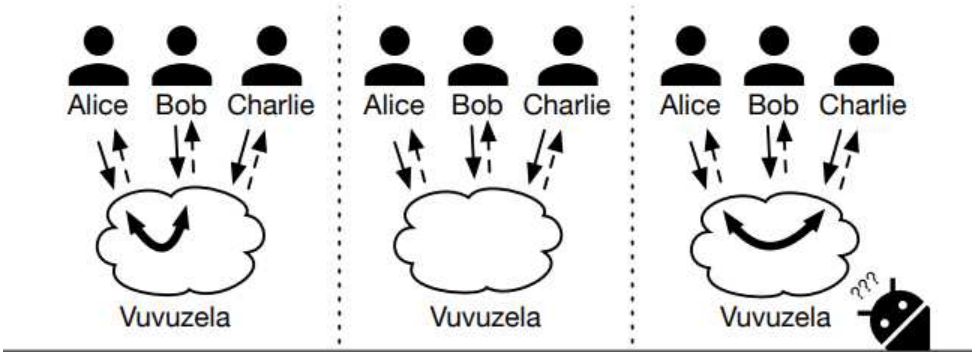


Figura 5 – Fluxo de privacidade do Vuvuzela.

Na Figura 5, o adversário não deve ser capaz de distinguir entre vários mundos possíveis. Em um mundo, Alice está se comunicando por meio do Vuvuzela com Bob. Em outro, ela está conectada, mas não troca mensagens com outros usuários. Em um terceiro, ela está se comunicando com Charlie. O Vuvuzela fornece à Alice Privacidade Diferencial: qualquer evento observado pelo adversário tem probabilidade aproximadamente igual em todos os mundos.

Os resultados experimentais demonstraram que o Vuvuzela possui um custo linear em relação ao número de clientes, o que o torna altamente escalável. Os testes realizados indicaram que o sistema pode alcançar uma taxa de transferência de 68.000 mensagens por segundo para 1 milhão de usuários, com uma latência de ponta a ponta de 37 segundos em servidores comuns. Esses resultados reforçam a eficácia e o desempenho do Vuvuzela como uma solução promissora para proteger a privacidade em sistemas de mensagens privadas em escala.

Em resumo, o trabalho apresenta o Vuvuzela como um sistema escalável e robusto que aborda os desafios da privacidade em mensagens privadas pela Internet. Ele oferece uma solução eficiente e resistente à análise de tráfego, garantindo a privacidade dos dados e metadados

das mensagens através da Prividade Diferencial. Os resultados experimentais confirmam a viabilidade e o bom desempenho do sistema, posicionando-o como uma alternativa valiosa para proteger a privacidade dos usuários em sistemas de mensagens em larga escala.

3.2 Privacy Preserving Classification Based on Perturbation for Network Traffic

O trabalho proposto por Lu *et al.* (2018) apresenta uma abordagem para a preservação da privacidade durante a classificação de dados de tráfego de rede, utilizando técnicas de seleção de atributos e anonimização dos dados. O estudo em questão baseia-se exclusivamente em dados de tráfego de rede de protocolos *TCP*. O objetivo principal é garantir que informações sensíveis presentes nos dados de tráfego não sejam reveladas durante o processo de classificação.

Uma das principais contribuições do trabalho é a utilização de técnicas de perturbação para proteger a privacidade dos dados. Essa abordagem consiste em adicionar um ruído controlado aos dados antes de realizar a classificação, de modo a dificultar a re-identificação de informações pessoais. A perturbação é aplicada de forma a preservar a utilidade dos dados, ou seja, permitir que a classificação ainda seja realizada com um nível aceitável de precisão.

Na etapa de seleção de atributos, o objetivo é identificar os atributos mais relevantes para a classificação dos dados de tráfego, mantendo a privacidade dos usuários. Nesse sentido, são aplicados métodos de seleção de atributos que levam em consideração critérios como a importância do atributo para a classificação e a sensibilidade dos dados. Técnicas como o ganho de informação, a razão de ganho e a correlação com a classe são também utilizadas para avaliar a relevância dos atributos e selecionar os mais adequados.

Após a seleção dos atributos, a etapa de anonimização dos dados é realizada com o objetivo de proteger a identidade dos usuários presentes no conjunto de dados de tráfego. O processo de perturbação é realizado da seguinte forma: primeiramente, é assumido que há um conjunto de dados de atributos brutos, representado por A, contendo n amostras. Em seguida, é gerado um novo conjunto de dados, representado por B, por meio da perturbação dos dados brutos. Ambos os conjuntos de dados têm o mesmo número de amostras (n).

Cada amostra contém m atributos, e cada atributo é representado por um vetor. Por exemplo, a n-ésima amostra de A é representada por $X_n = (x_n^1, x_n^2, x_n^3 ..., x_n^m)$, onde cada x_i representa o valor do atributo correspondente. De forma similar, a n-ésima amostra de B é representada por $Y_n = (y_n^1, y_n^2, y_n^3 ..., y_n^m)$, onde cada y_i representa o valor perturbado do atributo correspondente.

Uma das etapas importantes do método é a contagem da distribuição de cada atributo. Para ilustrar o processo, vamos considerar o primeiro atributo $P_1 = (x_1^1, x_2^1, x_3^1 ..., x_i^1, ..., x_n^1)$ em A. O objetivo é contar a distribuição desse atributo. Em vez de calcular a probabilidade para cada valor individual, é proposto dividir os valores em vários intervalos e calcular as funções de distribuição correspondentes a cada intervalo. Esse método simplifica o cálculo e melhora a generalidade da abordagem.

Para cada atributo, são realizados os seguintes passos: primeiro, encontra-se o valor máximo $(max(P_1))$ e o valor mínimo $(min(P_1))$ do atributo; em seguida, os dados no intervalo $[min(P_1), max(P_1)]$ são divididos uniformemente em k segmentos, obtendo assim os valores de partição; em seguida, é feita a contagem do número de dados em cada partição; finalmente, é aplicado o método de interpolação linear para obter as expressões das funções de distribuição correspondentes a cada partição.

Após a perturbação dos dados e a contagem da distribuição, é realizado o ajuste dos dados perturbados com base na relação de ordem entre os atributos. Esse processo tem como objetivo restaurar a correlação entre os dados o máximo possível. Para isso, é utilizado o exemplo de dois atributos, P_1 e P_2. As sequências geradas anteriormente (P_1 e P_2) são ajustadas com base na relação de ordem entre P_1 e P_2. O objetivo é manter os dados perturbados o mais próximo possível dos dados originais.

No final do processo, as sequências ajustadas são publicadas como dados perturbados para fins de pesquisa em classificação de tráfego. Esses dados publicados representam uma perturbação dos dados originais, garantindo a preservação da privacidade dos usuários e mantendo a utilidade dos dados através do algoritmo de perturbação baseado na relação de ordem.

Dessa forma, o método proposto neste trabalho combina a perturbação dos dados brutos com o ajuste baseado na relação de ordem para preservar a privacidade e a utilidade dos dados de tráfego de rede durante o processo de classificação.

3.3 ProTECting: Garantindo a privacidade de dados gerados em Casas Inteligentes localmente na Borda da rede

No trabalho Vidal *et al.* (2020), os autores propõem a utilização da Privacidade Diferencial como uma técnica para proteger a privacidade dos usuários em cenários de casas inteligentes na Internet das Coisas (IoT) na borda.

O trabalho apresenta uma técnica que trata cada dispositivo IoT em uma casa

inteligente como um agente individual. Cada agente coleta dados dos sensores e aplica um mecanismo de perturbação para adicionar ruído aos dados antes de compartilhá-los com outros dispositivos ou com uma entidade central. A perturbação dos dados é realizada de forma a preservar a privacidade dos usuários, tornando difícil a identificação de informações pessoais específicas.

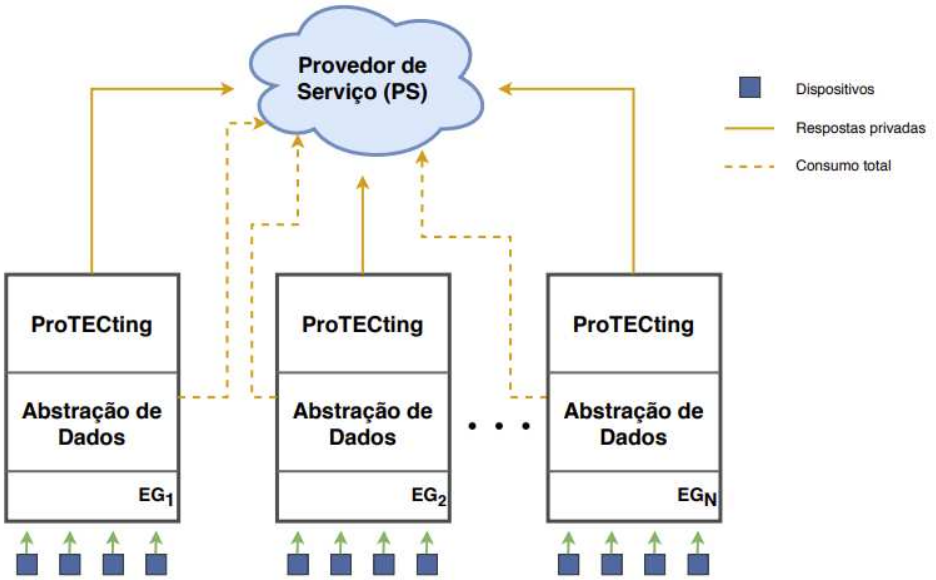


Figura 6 – Protecting – Comunicação entre o provedor de serviços e as casas.

Ao adicionar ruído aos dados coletados, a Privacidade Diferencial garante que os resultados agregados sejam consistentes e úteis, sem revelar informações sensíveis sobre indivíduos específicos. Dessa forma, a técnica protege a privacidade dos usuários, mesmo quando os dados são analisados em conjunto.

Além disso, o trabalho destaca a importância de considerar o contexto específico das casas inteligentes ao aplicar a Privacidade Diferencial. Isso inclui levar em conta a presença de múltiplos dispositivos na casa, a diversidade dos dados coletados e as características individuais dos sensores. A adaptação da técnica às particularidades das casas inteligentes é fundamental para garantir a eficácia e a utilidade dos resultados obtidos.

A técnica proposta no trabalho é avaliada por meio de experimentos e análises para medir a eficácia da técnica de Privacidade Diferencial. Os autores consideram métricas de privacidade, como a probabilidade de identificação de um indivíduo a partir dos resultados agregados, e métricas de utilidade, como a precisão dos resultados obtidos.

Os resultados demonstram que a técnica de Privacidade Diferencial pode proteger efetivamente a privacidade dos usuários em cenários de casas inteligentes, ao mesmo tempo em

que oferece resultados úteis e precisos para análise e tomada de decisões. A abordagem proposta representa uma solução promissora para equilibrar a privacidade dos usuários e o aproveitamento dos dados coletados em ambientes de IoT na borda, como as casas inteligentes.

3.4 Defeating Traffic Analysis via Differential Privacy: A Case Study on Streaming Traffic

O trabalho proposto por Zhang *et al.* (2022) apresenta uma abordagem inovadora baseada em Privacidade Diferencial para proteger a privacidade dos usuários durante a análise de tráfego de *streaming*. O objetivo principal do estudo é mitigar a capacidade de terceiros de realizar análises invasivas e identificar informações pessoais a partir do tráfego de dados de *streaming*.

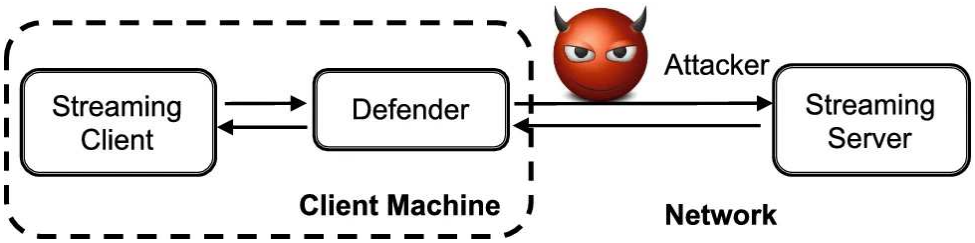


Figura 7 – Modelo de ameaça e identificação de informações pessoais a partir da análise do tráfego de dados de *streaming*.

A técnica proposta pelos autores envolve dois mecanismos principais: difusão e anonimização. Esses mecanismos são aplicados para dificultar a identificação de padrões específicos de tráfego e proteger a identidade dos usuários.

No contexto da difusão, os dados de tráfego são embaralhados para tornar mais difícil para um observador externo identificar informações sensíveis ou extrair padrões específicos do tráfego. Isso é realizado por meio da adição de ruído estatístico aos valores de tráfego, preservando ao mesmo tempo as características globais do tráfego. A difusão tem como objetivo principal tornar o tráfego de streaming menos identificável e mais anônimo, dificultando a correlação de pacotes de dados a indivíduos específicos.

Em relação à anonimização, o objetivo é proteger a identidade dos usuários. Para isso, informações pessoais identificáveis, como endereços IP ou identificadores de dispositivo, são removidas ou substituídas por pseudônimos ou valores genéricos. Isso impede que os observadores relacionem o tráfego a um indivíduo específico, garantindo assim a privacidade dos usuários. A anonimização é realizada de forma cuidadosa, levando em consideração a necessidade de preservar a utilidade dos dados para análises legítimas, ao mesmo tempo em que

protege a identidade dos usuários.

Os autores conduzem um estudo de caso usando tráfego de streaming real para avaliar a eficácia da abordagem proposta. Eles demonstram que a difusão e a anonimização dos dados de tráfego resultam em uma redução significativa na capacidade de um adversário de realizar análises invasivas e identificar informações pessoais. Além disso, eles avaliam a utilidade e a segurança das técnicas propostas, garantindo que a proteção da privacidade não comprometa a qualidade e a utilidade dos dados para fins legítimos.

Em resumo, a abordagem proposta neste trabalho utiliza os mecanismos de difusão e anonimização para proteger a privacidade dos usuários durante a análise de tráfego de streaming. A difusão envolve o embaralhamento dos dados de tráfego por meio da adição de ruído estatístico, enquanto a anonimização protege a identidade dos usuários, removendo ou substituindo informações pessoais identificáveis. O estudo de caso realizado pelos autores demonstra a eficácia e a utilidade desses mecanismos na proteção da privacidade dos usuários, ao mesmo tempo em que garantem a segurança e a qualidade dos dados para análises legítimas.

3.5 Discussão

Diversas abordagens têm sido propostas na literatura para a preservação da privacidade em relação aos dados de tráfego de rede. Em particular, o trabalho de Hooff *et al.* (2015), chamado de Vuvuzela, propõe um novo sistema de mensagens privadas escalável, capaz de resistir à análise de tráfego de rede com base na Privacidade Diferencial. Contudo, a abordagem proposta apresenta um custo computacional elevado, significando que ele pode exigir mais recursos computacionais para processar e transmitir as mensagens, o que pode levar a um desempenho inferior em termos de latência e *throughput* em comparação com a abordagem proposta neste trabalho *DPNetTraffic*.

Deve-se também levar em consideração a complexidade da sua implementação, o que pode dificultar o desenvolvimento e a manutenção do sistema. Além disso, essa complexidade aumenta a possibilidade de erros e vulnerabilidades de segurança, representando um desafio adicional para garantir a robustez do sistema. Uma outra desvantagem do Vuvuzela é sua dependência de um único servidor confiável. Isto é, todo o sistema fica vulnerável caso esse servidor seja comprometido, representando um ponto de falha centralizado. É importante mencionar que o Vuvuzela opera no nível de serviços, enquanto o *DPNetTraffic* aplica-se nos níveis de portas, protocolos e serviços.

O trabalho Lu *et al.* (2018) apresenta um método que visa proteger informações sensíveis presentes nos dados de tráfego, ao mesmo tempo em que permite a sua classificação para análise de segurança. A abordagem proposta neste estudo baseia-se na utilização da técnica de perturbação, que consiste na perturbação das informações de tráfego antes da etapa de classificação.

Os resultados obtidos a partir de experimentos demonstram a eficácia do método em preservar a privacidade das informações de tráfego, ao mesmo tempo em que proporciona resultados de classificação precisos. Contudo, é importante ressaltar que o referido trabalho não incorpora garantias formais fundamentadas na noção de Privacidade Diferencial, o que resulta em uma definição de privacidade menos rigorosa.

Uma possível melhoria para o trabalho seria a adoção de uma abordagem baseada em Privacidade Diferencial, que é uma técnica estabelecida e amplamente reconhecida para a proteção da privacidade em conjuntos de dados. Ao incorporar essa abordagem, seria possível quantificar e controlar o nível de informação sensível revelada durante o processo de classificação dos dados de tráfego de rede. Dessa forma, seriam estabelecidos limites aceitáveis de divulgação de informações sensíveis, garantindo uma proteção mais robusta da privacidade dos usuários.

Em Vidal *et al.* (2020), os autores propõem a utilização da Privacidade Diferencial como uma técnica para proteger a privacidade dos usuários em cenários de casas inteligentes. O trabalho apresenta uma técnica que trata cada dispositivo em uma casa inteligente como um agente individual.

Embora o trabalho destaque a importância de considerar a presença de múltiplos dispositivos na casa, a diversidade dos dados coletados e as características individuais dos sensores, é necessário aprofundar a análise e desenvolver abordagens mais robustas para lidar com as especificidades do tráfego de redes. Além disso, há uma necessidade de adaptar a técnica às particularidades das casas inteligentes e ao contexto do tráfego de redes de computadores, uma vez que os provedores de serviço de internet (ISPs) são os responsáveis por consolidar e gerenciar esse tráfego na borda da rede. Aperfeiçoar a técnica para lidar com o contexto do tráfego de redes de computadores, considerando aspectos como a natureza dinâmica dos dados e a proteção contra ataques sofisticados, será crucial para fortalecer a privacidade dos usuários.

O trabalho proposto por Zhang *et al.* (2022) apresenta uma abordagem inovadora que atende à Privacidade Diferencial para proteger a privacidade dos usuários durante a análise de tráfego de streaming. O principal objetivo do estudo é mitigar a capacidade de terceiros de

realizar análises invasivas e identificar informações pessoais a partir do tráfego de dados em tempo real.

A técnica proposta pelos autores envolve dois mecanismos principais: difusão e anonimização. Esses mecanismos são aplicados para dificultar a identificação de padrões específicos de tráfego e proteger a identidade dos usuários.

Uma das limitações é a necessidade de encontrar um equilíbrio entre a difusão dos dados de tráfego e a preservação da utilidade dos mesmos. A adição de ruído estatístico pode dificultar a identificação de informações sensíveis, mas também pode afetar a precisão e a qualidade dos resultados da análise. Portanto, é essencial realizar estudos adicionais para avaliar o impacto da difusão nos dados e a adequação dos resultados obtidos, garantindo a utilidade dos dados para fins de análise.

Além disso, é importante considerar que a eficácia da abordagem proposta pode depender do cenário de tráfego de streaming em que está sendo aplicada. Diferentes contextos de tráfego podem apresentar desafios específicos que exigem ajustes e adaptações na técnica de preservação da privacidade. Portanto, é necessário investigar mais a fundo a generalização e a robustez da abordagem proposta em diferentes contextos de tráfego de rede.

A nossa contribuição, chamada de *DPNetTraffic*, destaca-se como uma solução eficaz, apresentando menor custo computacional e melhor desempenho em comparação com outras abordagens, como o Vuvuzela (HOOFF *et al.*, 2015), que possui um alto custo computacional e dependência de um único servidor confiável. O trabalho de Lu *et al.* (2018) aborda a proteção da privacidade no tráfego de rede por meio da perturbação dos dados, mas não incorpora garantias formais baseadas em Privacidade Diferencial. Já o trabalho de Vidal *et al.* (2020) propõe o uso da Privacidade Diferencial para proteger a privacidade dos usuários em casas inteligentes, mas requer adaptação para lidar com o contexto do tráfego de redes. Os autores Zhang *et al.* (2022) propõem uma abordagem inovadora para proteger a privacidade durante a análise de tráfego de *streaming*, porém, a eficácia da técnica pode variar dependendo do cenário de tráfego em que é aplicada. O *DPNetTraffic* apresenta uma estratégia para proteger a privacidade em diferentes níveis no contexto de tráfego de redes satisfazendo à Privacidade Diferencial, fornecendo um equilíbrio entre privacidade, desempenho e utilidade dos dados. A Tabela 2 apresenta um resumo comparativo entre os trabalhos apresentados neste capítulo e a abordagem que compõe nossa contribuição, o *DPNetTraffic*.

Trabalho	Estratégia de Privacidade	Portas	Protocolos	Serviços
Hooff *et al.* (2015)	Privacidade Diferencial			✓
Lu *et al.* (2018)	Perturbação		✓	
Vidal *et al.* (2020)	Privacidade Diferencial			✓
Zhang *et al.* (2022)	Privacidade Diferencial			✓
DPNetTraffic	Privacidade Diferencial	✓	✓	✓

Tabela 2 – Tabela comparativa de trabalhos relacionados.

3.6 Conclusão

Neste capítulo, foram expostos os principais estudos que se relacionam com o tema abordado nesta dissertação. Os trabalhos apresentados fornecem uma base sólida de conhecimento e investigação no campo de estudo em questão, abordando diversos aspectos e tópicos relevantes. Apesar dos estudos realizados nos trabalhos mencionados anteriormente, nenhum deles foca no compartilhamento de informações privadas do trafego de rede, em particular portas, protocolos e serviços. A seguir, apresentamos o *DPNetTraffic*, uma nova técnica que permite aos provedores de serviço internet (ISPs) e entidades que coletam dados de tráfego de rede compartilharem, ou comercializarem, seus dados por meio da Privacidade Diferencial.

4 METODOLOGIA

No capítulo anterior, foram apresentados e discutidos trabalhos relevantes que se concentram no contexto do tráfego de redes. Neste Capítulo, apresentaremos o *DPNetTraffic*, uma nova técnica que permite aos provedores de serviço de internet e entidades que coletam dados de tráfego de rede compartilharem, ou comercializarem, seus dados por meio da Privacidade Diferencial. Inicialmente nós pré-processamos o conjunto de dados original, agrupando-os por portas, protocolos e serviços, conforme registro de dados de tráfego de rede disponibilizado publicamente pela IANA[1] (*Internet Assigned Numbers Authority*), organização responsável por coordenar a alocação global de recursos relacionados à Internet (IANA, 2023). Em seguida, nós aplicamos a Privacidade Diferencial sobre a contagem dos registros agrupados a fim de perturbá-los. Por fim, nós propomos uma técnica de pós-processamento para agrupar as contagens sobre os dados ruidosos, remover as contagens negativas e assim garantir a utilidade das informações após todo o processo.

4.1 Relevância das Consultas de Contagem

Contagens são um objeto natural de estudo para análise de dados no contexto de preservação da privacidade (MACHANAVAJJHALA *et al.*, 2017). Elas permitem que os usuários computem o número de indivíduos em um conjunto de dados que atendem a determinados predicados, sem revelar informações sensíveis sobre os indivíduos em si. Diversas consultas de contagem podem ser realizadas, como a construção de histogramas, a definição de intervalos em consultas de alcance (*range queries*) e a obtenção de funções de distribuição cumulativas, entre outras (LI *et al.*, 2010).

Essas consultas são essenciais para a compreensão e análise dos dados, permitindo extrair informações estatísticas relevantes. Ao aplicar a Privacidade Diferencial às consultas de contagens, é possível adicionar ruído estatístico aos resultados, garantindo que as informações divulgadas sejam agregadas e dificultando a identificação direta ou indireta de indivíduos específicos (NISSIM *et al.*, 2007). Consequentemente, ao publicar consultas de contagens de maneira privada, entidades que coletam dados podem realizar uma série de análises importantes sobre os dados sem comprometer a privacidade dos indivíduos pertencentes a eles. Nas seções a seguir exemplificamos as respostas de consultas de contagem propostas neste trabalho.

[1] https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

4.1.1 Contagem de Portas

A contagem de portas de rede é uma prática comum na análise de tráfego de rede e é um processo importante para entender quais serviços e protocolos estão sendo utilizados em uma determinada rede (PETERSON; DAVIE, 2007). Existem algumas portas que são comumente usadas para serviços específicos, como a porta 80 para o serviço HTTP (*Hypertext Transfer Protocol*) e a porta 443 para o serviço *HTTPS* (*HTTP Secure*) (IANA, 2023).

Os números de porta são atribuídos de várias maneiras, com base em três faixas: Portas do Sistema ($0 - 1023$), Portas de Usuário ($1024 - 49151$) e as Portas Dinâmicas e/ou Privadas ($49152 - 65535$); os diferentes usos dessas faixas são descritos em Cotton *et al.* (2023). No entanto, algumas portas podem ser usadas para diferentes serviços ou podem ser atribuídas a serviços personalizados criados pelos usuários. Por isso, é importante analisar quais serviços estão sendo executados em cada porta para obter uma compreensão completa do tráfego de rede.

Em particular, a análise do tráfego de rede e a contagem das portas utilizadas podem ser úteis na identificação dos aplicativos e serviços em uso na rede. Essa informação tem diversas aplicações, como o gerenciamento da rede, a segurança e a solução de problemas (KUROSE *et al.*, 2013). Ao contar as portas em uso, é possível obter informações úteis sobre o tráfego de dados, identificar potenciais gargalos, monitorar o uso de aplicativos específicos e detectar atividades maliciosas. Essa análise detalhada das portas ajuda a otimizar o desempenho da rede, garantir a conformidade com as políticas de segurança e facilitar a resolução de problemas relacionados à conectividade e disponibilidade dos serviços.

Por exemplo, se um administrador de rede perceber um aumento no tráfego da porta 80, ele pode suspeitar que há um aumento no uso da web na rede. Se o aumento for excessivo, ele pode considerar a possibilidade de limitar o acesso à internet para evitar sobrecarregar a rede. Além disso, a contagem de portas pode ajudar a identificar atividades maliciosas na rede, como tráfego de malware ou tentativas de invasão. Se um grande número de conexões estiver sendo feito a uma porta específica, pode indicar um ataque em andamento.

Em suma, a contagem de portas é uma técnica útil na análise de tráfego de rede, permitindo que administradores de rede identifiquem aplicativos e serviços em uso, gerenciem o tráfego da rede e detectem atividades maliciosas.

4.1.2 Contagem de Protocolos

A contagem de protocolos de redes refere-se à contagem do número de conexões estabelecidas usando protocolos de transporte como *TCP* (*Transmission Control Protocol*) e *UDP* (*User Datagram Protocol*). O *TCP* e *UDP* são dois dos protocolos de transporte mais comuns utilizados em redes de computadores (KUROSE *et al.*, 2013). Para fins de referência, nos conjuntos de dados utilizados neste trabalho, existem apenas conexões *TCP* e *UDP*.

O protocolo *TCP* é amplamente utilizado em redes de computadores como um protocolo orientado a conexão. Ele oferece mecanismos de confiabilidade, controle de fluxo e controle de congestionamento para garantir a entrega confiável e ordenada dos dados transmitidos (TANENBAUM; WETHERALL, 2021). Em contraste, o protocolo *UDP* é um protocolo não orientado a conexão, no qual os pacotes são enviados de forma independente, sem garantias de entrega ou controle de fluxo (TANENBAUM; WETHERALL, 2021).

A contagem das conexões baseadas nos protocolos *TCP* e *UDP* pode ser uma estratégia valiosa para o monitoramento do tráfego de redes. Ao analisar a quantidade de conexões *TCP* e *UDP* estabelecidas, é possível obter informações sobre a utilização dos serviços e aplicativos na rede (KUROSE *et al.*, 2013; TANENBAUM; WETHERALL, 2021). Essa informação pode ser usada para identificar gargalos de desempenho, otimizar o uso de recursos de rede e alocar largura de banda de forma adequada.

Além disso, a contagem de protocolos também pode ser útil para fins de segurança, permitindo identificar possíveis ameaças ou atividades suspeitas na rede. Por exemplo, alguns tipos de ataques, como o Denial of Service (DoS), geralmente usam protocolos específicos para sobrecarregar os recursos da rede. Ao monitorar a quantidade de tráfego gerado por cada protocolo, é possível identificar padrões de uso incomuns e tomar medidas para mitigar possíveis ataques (TANENBAUM; WETHERALL, 2021).

Portanto, a contagem das conexões TCP e UDP é uma prática essencial para a identificação de problemas de desempenho e a detecção de atividades suspeitas. Essa abordagem fornece informações valiosas para a administração da rede, permitindo a tomada de decisões embasadas em dados e a implementação de medidas de segurança eficazes.

4.1.3 Contagem de Serviços

A contagem proveniente dos fluxos de rede para serviços é particularmente importante para auxiliar administradores a rastrearem o uso da rede por diferentes departamentos ou usuários, o que pode ser útil para fins de faturamento ou para identificar possíveis violações de políticas de uso da rede (TANENBAUM; WETHERALL, 2021). Dessa forma, é possível responder a perguntas, de maneira privada, do tipo: *"qual serviço de streaming é mais utilizado?"*.

A contagem de serviços de rede desempenha um papel crucial na análise e gerenciamento do tráfego de rede. Essa prática envolve a identificação e classificação dos serviços mais comuns que utilizam protocolos de transporte específicos, como o *TCP* e o *UDP* (KUROSE *et al.*, 2013). Essa abordagem permite obter uma visão abrangente dos serviços em uso na rede e entender melhor como os recursos de rede estão sendo utilizados.

Ao realizar a contagem de serviços, é possível identificar os aplicativos e serviços específicos que estão sendo consumidos na rede. Por exemplo, pode-se contar o número de conexões estabelecidas para serviços como HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), entre outros. Esses dados fornecem informações valiosas sobre o tráfego de rede e permitem a administração eficiente da infraestrutura de rede.

Existem várias listas disponíveis que classificam os serviços de rede por protocolo e portas, incluindo a lista de serviços da IANA (Internet Assigned Numbers Authority) (IANA, 2023), que é usada como referência padrão para muitas aplicações e sistemas de rede. A lista da IANA inclui centenas de serviços diferentes, como *HTTP* (porta 80), *FTP* (porta 21), *SSH* (porta 22), *DNS* (porta 53), entre outros (COTTON *et al.*, 2023).

Além disso, a contagem de serviços auxilia as empresas a dimensionar e gerenciar a rede adequadamente, aplicar políticas de QoS, gerenciar o desempenho e detectar atividades maliciosas (TANENBAUM; WETHERALL, 2021). Isso garante que os serviços sejam entregues de forma confiável e segura para os usuários.

4.2 DPNetTraffic

Como mencionado, este trabalho propõe uma nova técnica para permitir aos provedores de serviço de internet e entidades que coletam dados de tráfego de rede compartilharem, ou comercializarem, seus dados por meio da privacidade diferencial. Este trabalho visa publi-

car (compartilhar) o resultado de três contagens distintas de maneira privada. Em particular a contagem de portas de destino, de protocolos utilizados e de serviços dos fluxos de rede.

A abordagem mais usual para contornar esse tipo de problema é aplicar diretamente a privacidade diferencial através do mecanismo geométrico sobre cada uma das três consultas de contagem (DWORK, 2006). Como discutido na Seção 2.3.5.2, o mecanismo geométrico é uma variante discreta do mecanismo de Laplace, o qual é frequentemente empregado em consultas envolvendo respostas de números inteiros, no caso deste trabalho, consultas de contagem. Em outras palavras, para cada contagem de portas de destino, protocolos e serviços, um ruído estatístico é adicionado com base na distribuição geométrica simétrica (Teorema 2).

Contudo, como três contagens distintas necessitam ser obtidas sobre o mesmo conjunto de dados, o orçamento de privacidade ε deve ser dividido por três (Definição 4). Isso faz com que o mecanismo geométrico produza saídas com ruídos maiores e, consequentemente, contagens com maiores erros. Esses resultados são apresentados no Capítulo 5.

Para lidar com o problema de compartilhamento de dados de tráfego de rede de maneira privada, nós propomos uma abordagem baseada em três etapas:

1. pré-processamento do conjunto de dados original com base em informações públicas;
2. aplicação do Mecanismo Geométrico sobre os dados pré-processados;
3. ajuste das contagens negativas e agrupamento das contagens a partir dos dados ruidosos.

A Figura 8 demonstra o *pipeline* de anonimização do *DPNetTraffic*. Desde os dados originais de tráfego de rede até o compartilhamento ruidoso das contagens. Na Figura 8a, temos o conjunto de dados original. Na Figura 8b, são mostrados os dados pré-processados juntamente com suas contagens originais. Na Figura 8c, temos o conjunto de dados agregado juntamente com sua contagem ruidosa. Por fim, na Figura 8d, é apresentada a contagem ruidosa dos serviços, portas e protocolos.

4.2.1 Pré-processamento dos Dados

O objetivo do pré-processamento é agrupar os dados de tal sorte que a adição de ruído, via Privacidade Diferencial, seja executada apenas uma vez, ao invés de três vezes seguindo a abordagem mais usual. Essa estratégia evita que o orçamento de privacidade seja dividido (Definição 4) e, consequentemente, produz contagens mais próximas das originais.

O Algoritmo 1 exemplifica os passos do pré-processamento da nossa abordagem. Inicialmente, a partir do conjunto de dados original, o IP de destino é removido (linha 1), por ser

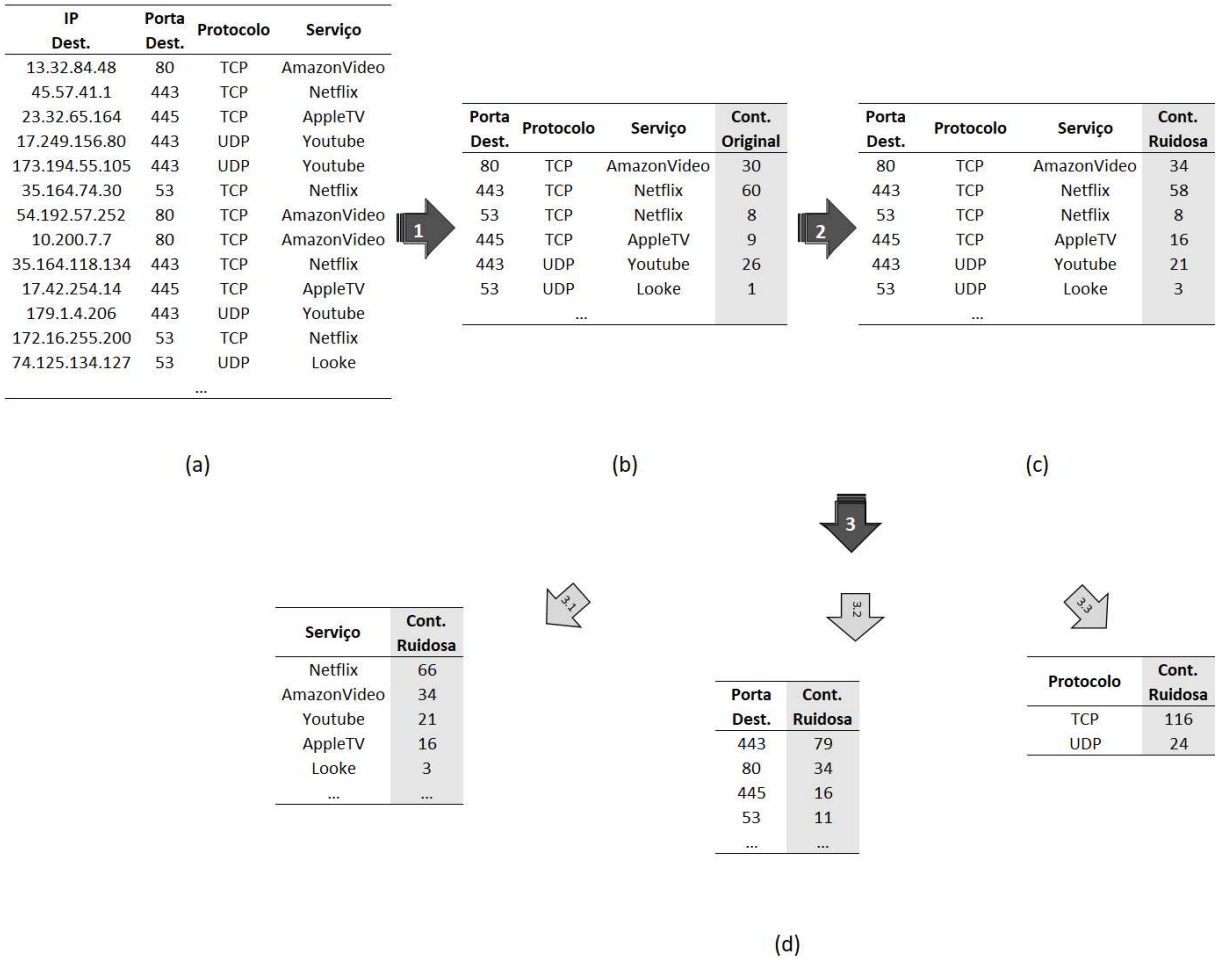


Figura 8 – *Pipeline* de anonimização do *DPNetTraffic*

um identificador explícito. Já na linhas 2 e 3, os dados originais são agrupados por triplas (porta, protocolo e serviço). Essa etapa de agrupamento é realizada com base nos registros de dados de tráfego de rede disponibilizados publicamente pela Internet Assigned Numbers Authority (IANA, 2023), organização responsável por coordenar a alocação global de recursos relacionados à Internet.

Em outras palavras, a IANA mantém um registro de portas, de protocolo e serviços atribuídos, que inclui informações sobre os protocolos associados a essas portas e os serviços que eles fornecem. A IANA formaliza esse registro através da [*RFC6335*[2]]. Assim, é possível agrupar os dados com base nessas informações sem ferir a privacidade dos indivíduos, visto que essas informações são de domínio público (COTTON *et al.*, 2023).

Para cada tripla agrupada com base nos padrões da IANA, suas respectivas contagens são calculadas no conjunto de dados original (linha 4). É importante ressaltar que essas contagens são informações privadas e sensíveis e, uma vez compartilhadas sem garantias formais de

[2] https://www.rfc-editor.org/rfc/rfc6335.html

privacidade, podem levar à re-identificação de indivíduos no conjunto de dados original. A Figura 9 apresenta um exemplo do conjunto de dados original pré-processado com suas respectivas contagens.

IP Dest.	Porta Dest.	Protocolo	Serviço
13.32.84.48	80	TCP	AmazonVideo
45.57.41.1	443	TCP	Netflix
23.32.65.164	445	TCP	AppleTV
17.249.156.80	443	UDP	Youtube
173.194.55.105	443	UDP	Youtube
35.164.74.30	53	TCP	Netflix
54.192.57.252	80	TCP	AmazonVideo
10.200.7.7	80	TCP	AmazonVideo
35.164.118.134	443	TCP	Netflix
17.42.254.14	445	TCP	AppleTV
179.1.4.206	443	UDP	Youtube
172.16.255.200	53	TCP	Netflix
74.125.134.127	53	UDP	Looke
...			

(a)

Porta Dest.	Protocolo	Serviço	Cont. Original
80	TCP	AmazonVideo	30
443	TCP	Netflix	60
53	TCP	Netflix	8
445	TCP	AppleTV	9
443	UDP	Youtube	26
53	UDP	Looke	1
...			

(b)

Figura 9 – (a) Conjunto de dados original. (b) Conjunto de dados pré-processados e suas respectivas contagens originais.

Algoritmo 1 Pré-Processamento

Entrada: Conjunto de dados $\mathscr{D}$.
Saída: Contagem do conjunto de dados agrupado $\hat{\mathscr{D}}$.
1: $\mathscr{D} \leftarrow$ remover('IP DE DESTINO')
2: $atributos \leftarrow$ ['PORTA DE DESTINO', 'PROTOCOLO', 'SERVIÇO']
3: $agrupamentos \leftarrow$ agrupar($\mathscr{D}$, $atributos$)
4: $\hat{\mathscr{D}} \leftarrow$ contar($agrupamentos$)
5: **Retorno:** $\hat{\mathscr{D}}$

4.2.2 Aplicação do Mecanismo Geométrico

Após o pré-processamento, o mecanismo Geométrico é aplicado sobre as contagens de cada tripla pré-processada na fase anterior. A aplicação do mecanismo Geométrico é descrita no Algoritmo 2. Esse processo envolve a introdução de ruído aleatório na contagem original calibrada pelo orçamento de privacidade ε e pela sensibilidade global Δq (linhas 1-3). Dessa forma, a privacidade dos dados é formalmente garantida. A Figura 10 mostra os dados agrupados anteriormente, agora com suas respectivas contagens ruidosas.

Algoritmo 2 Aplicação do Mecanismo Geométrico

Entrada: Conjunto de dados $\mathscr{D}$ e orçamento de privacidade ε.
Saída: Conjunto de dados diferencialmente privado $\tilde{\mathscr{D}}$.

1: $\alpha \leftarrow e^{-\varepsilon}$
2: $\hat{\mathscr{D}} \leftarrow$ Pré-Processamento($\mathscr{D}$)
3: $\tilde{\mathscr{D}} \leftarrow \hat{\mathscr{D}}$ + Geométrico(α)
4: **Retorno:** $\tilde{\mathscr{D}}$

Porta Dest.	Protocolo	Serviço	Cont. Original
80	TCP	AmazonVideo	30
443	TCP	Netflix	60
53	TCP	Netflix	8
445	TCP	AppleTV	9
443	UDP	Youtube	26
53	UDP	Looke	1
	...		

Porta Dest.	Protocolo	Serviço	Cont. Ruidosa
80	TCP	AmazonVideo	34
443	TCP	Netflix	58
53	TCP	Netflix	8
445	TCP	AppleTV	16
443	UDP	Youtube	21
53	UDP	Looke	3
	...		

(b) (c)

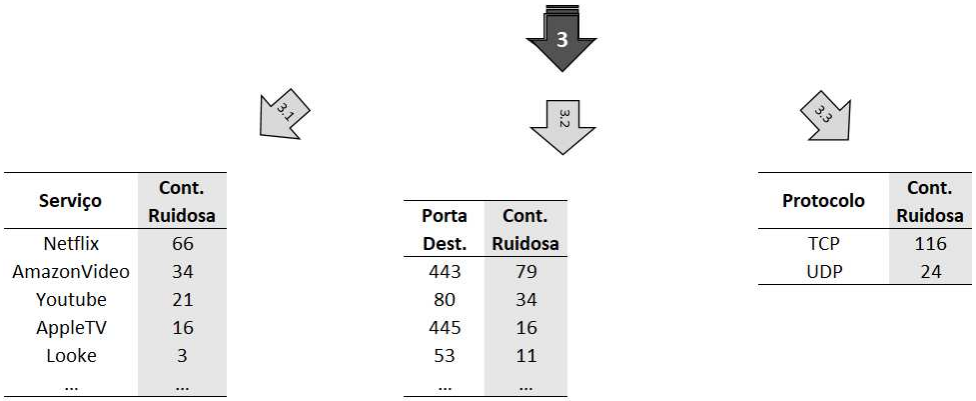
Figura 10 – (b) Conjunto de dados pré-processados e suas respectivas contagens originais. (c) Conjunto de dados agregado e sua contagem ruidosa.

No exemplo em questão, para a tripla (80, TCP, AmazonVideo) um ruído de valor 4 foi adicionado à contagem original. Já para a tripla (443, TCP, Netflix) um ruído de valor -2 foi acrescentado ao dado original. Já para a tripla (53, TCP, Netflix) um ruído de valor 0 foi introduzido, isto é, o dado permaneceu o mesmo.

Pelo fato do ruído adicionado aos dados ser aleatório, um usuário malicioso que tem acesso aos dados compartilhados não possui conhecimento de quais contagens foram alteradas e quais permaneceram as mesmas, e nem a quantidade de ruído introduzido em cada contagem.

4.2.3 Pós-processamento

Finalmente, após adição de ruído aos dados, uma etapa de pós-processamento é conduzida a fim de obter as contagens agregadas por portas de destino, protocolos e serviços, isto é, o objetivo final da nossa abordagem. Esta etapa é descrita no Algoritmo 3 (linhas 1-6). A Figura 11 apresenta os dados de contagem de serviços, portas destino e protocolos agregados pela soma de suas contagens ruidosas.



(d)

Figura 11 – (d) Contagem ruidosa de serviços, portas e protocolos.

Algoritmo 3 Pós-processamento

Entrada: Conjunto de dados diferencialmente privado $\tilde{\mathscr{D}}$.
Saída: Contagens agregadas por $\tilde{\mathscr{D}}_{porta}$, $\tilde{\mathscr{D}}_{protocolo}$, $\tilde{\mathscr{D}}_{servico}$.

1: $agrupamentos\_portas \leftarrow$ agrupar($\tilde{\mathscr{D}}$[‘PORTA DE DESTINO’])
2: $\tilde{\mathscr{D}}_{porta} \leftarrow$ Contar($agrupamentos\_portas$)
3: $agrupamentos\_protocolo \leftarrow$ agrupar($\tilde{\mathscr{D}}$[‘PROTOCOLO’])
4: $\tilde{\mathscr{D}}_{protocolo} \leftarrow$ contar($agrupamentos\_protocolo$)
5: $agrupamentos\_servico \leftarrow$ agrupar($\tilde{\mathscr{D}}$[‘SERVICO’])
6: $\tilde{\mathscr{D}}_{servico} \leftarrow$ contar($agrupamentos\_servico$)
7: **Retorno:** $\tilde{\mathscr{D}}_{porta}, \tilde{\mathscr{D}}_{protocolo}, \tilde{\mathscr{D}}_{servico}$

Além disso, ao compartilhar uma determinada contagem, seja de qualquer tipo, o *DPNetTraffic* pode retornar um valor negativo devido à adição de ruído aleatório pelo Mecanismo Geométrico ser tanto positiva quanto negativa (Teorema 2). Nosso pós-processamento arredonda os valores agregados de contagem negativa para o menor valor inteiro positivo possível, isto é, arredonda-se para 1 (um).

É importante ressaltar que a etapa de pós-processamento não viola as garantias formais da Privacidade Diferencial, uma vez que qualquer função aplicada a um conjunto de dados que já é diferencialmente privado também satisfaz à Privacidade Diferencial (Definição 3).

4.2.3.1 Ajuste das Contagens Negativas

A Privacidade Diferencial adiciona ruído, calibrado pelo orçamento de privacidade ε e pela sensibilidade Δq, aos resultados numéricos de uma consulta antes de retorná-los. No entanto, esse processo pode afetar algumas restrições de domínio. Por exemplo, ao consultar

a contagem de uma determinada porta, um valor de resposta negativo pode ser retornado. Na prática, contagens não exibem valores negativos, ou seja, respostas a consultas de contagem devem estar no domínio dos inteiros positivos $\mathbb{Z}_{>0}$. A adição de ruído aleatório pelo mecanismo Geométrico não pode garantir tal restrição, devido ao ruído inserido por esse mecanismo ser tanto positivo quanto negativo (Teorema 2).

Uma solução simples para lidar com contagens negativas é limitar esses valores em 1. Entretanto, isso introduz tendência nos dados. Observe que, devido ao mecanismo Geométrico possuir média 0, o somatório final das contagens ruidosas, em expectativa, é igual ao somatório das contagens originais. A Figura 10 exemplifica esse fato. A contagem de registros que utilizam TCP via mecanismo Geométrico é muito próxima da contagem original. Ao limitar os valores negativos em 1, as contagens computadas após Mecanismo Geométrico passam a ter somatório maior que o somatório das contagens originais, visto que valores negativos ganham unidades para se tornarem positivos. É nesse ponto que a tendência é introduzida.

Na literatura existe um mecanismo $\mathscr{M}$, denominado Log-Laplace (NY; PAPPAS, 2013) e discutido no Seção 2.3.5.3, que evita inserir ruído negativo aos dados. Contudo, diferentemente dessa abordagem, nós propomos ajustar as contagens negativas preservando seu somatório após aplicação do ruído geométrico. Para isso, modelamos e solucionamos um problema de otimização inteira conforme descrito abaixo. Essa etapa do pós-processamento é descrito no Algoritmo 4.

Algoritmo 4 Ajuste de Contagens Negativas

Entrada: Conjunto de dados diferencialmente privado $\tilde{\mathscr{D}}$
Saída: Conjunto de dados diferencialmente privado $\bar{\mathscr{D}}$ sem contagens negativas.
1: $\bar{\mathscr{D}} = \tilde{\mathscr{D}}$
2: $funcao\_custo \leftarrow \min_{\bar{\mathscr{D}}} ||\bar{\mathscr{D}} - \tilde{\mathscr{D}}||_2^2$
3: $restricao_1 \leftarrow \bar{\mathscr{D}} \in \mathbb{Z}_{>0}$
4: $restricao_2 \leftarrow \sum_{i=1}^{n} \bar{\mathscr{D}}_i \leftarrow \sum_{i=1}^{n} \tilde{\mathscr{D}}_i$
5: $\tilde{\mathscr{D}} \leftarrow$ CVXPY($\bar{\mathscr{D}}$, $\tilde{\mathscr{D}}$, $funcao\_custo$, $restricao_1$, $restricao_2$)
6: **Retorno:** $\bar{\mathscr{D}}$

Considere a saída ruidosa de uma consulta de contagem diferencialmente privada $\tilde{\mathscr{D}}$, seja ela de porta, protocolo ou serviço. Nós visamos encontrar uma solução $\bar{\mathscr{D}}$ (linha 1) que minimiza a distância ao quadrado l_2 (linha 2) para a resposta ruidosa $\tilde{\mathscr{D}}$, isto é, uma solução mais próxima possível da desejada, que retorna valores inteiros positivos (linha 3) e que também preserva o somatório das contagens em $\tilde{\mathscr{D}}$ (linha 4). Dessa forma, modelamos o seguinte

problema de otimização:

$$\min_{\bar{\mathscr{D}}} ||\bar{\mathscr{D}} - \tilde{\mathscr{D}}||_2^2 \tag{4.1}$$

tal que $\bar{\mathscr{D}} \in \mathbb{Z}_{>0}$ e $\sum_{\mathrm{i}=1}^{n} \bar{\mathscr{D}}_{\mathrm{i}} = \sum_{\mathrm{i}=1}^{n} \tilde{\mathscr{D}}_{\mathrm{i}}$,

Para solucionar este problema, aplicamos uma técnica de otimização fundamentada na programação inteira, como discutido por Agrawal *et al.* (2018). A programação inteira é uma classe de problemas de otimização em que algumas ou todas as variáveis devem ser números inteiros. Dessa forma, as contagens compartilhadas com entidades externas atendem à restrição $\mathbb{Z}_{>0}$ e preservam o somatório das contagens originais (linha 5 e 6).

Após a realização do ajuste das contagens negativas, observa-se uma melhora no desempenho do algoritmo *DPNetTraffic*. Como resultado dessa melhoria, é gerado o *DPNetTraffic + PostProcessing*, que incorpora uma menor quantidade de ruído aos dados, aumentando a utilidade e a precisão no processo de análise desses dados.

4.3 Conclusão

Este capítulo apresentou o *DPNetTraffic*, uma nova técnica que permite a provedores de serviço de internet (ISP) e entidades que coletam dados de tráfego de rede publicar dados de tráfego de rede com garantias formais de privacidade. Inicialmente, agrupamos os dados em triplas contendo portas, protocolos e serviços, para que a adição de ruído fosse executada apenas uma vez, ao invés de três vezes utilizando a abordagem mais usual da Privacidade Diferencial. Em seguida, o Mecanismo Geométrico foi aplicado sobre as contagens de cada tripla pré-processada, a fim de introduzir ruído aleatório na contagem original. Por fim, obtemos as contagens agregadas por portas de destino, protocolos e serviços via pós-processamento de dados, isto é, o objetivo final da nossa abordagem. Na etapa de pós-processamento também propomos uma solução para lidar com contagens negativas produzidas pela segunda etapa da nossa abordagem, limitando os valores em 1. Com isso em vista, o *DPNetTraffic* foi aprimorado para *DPNetTraffic* + PostProcessing atingindo um melhor desempenho ao adicionar menos ruído aos dados anonimizados de até $57,4\%$ para contagens de portas, $26,55\%$ para contagem de serviços e até $9,93\%$ para contagem de protocolos. Resultados de ambas as abordagens, *DPNetTraffic* e *DPNetTraffic + PostProcessing*, podem ser vistos no capítulo a seguir.

5 AVALIAÇÃO EXPERIMENTAL

No capítulo anterior, apresentamos o *DPNetTraffic*, *DPNetTraffic + PostProcessing* e seu *pipeline* de anonimização que satisfazem à Privacidade Diferencial. Neste Capítulo, serão apresentados seus resultados experimentais. Inicialmente, na Seção 5.1, o ambiente de execução é apresentado. Em seguida, na Seção 5.2, descrevemos os conjuntos de dados utilizados nos experimentos. Posteriormente, explicamos como é feita a análise de utilidade, detalhando as métricas que são utilizadas na Seção 5.3. Por último, são apresentados os resultados obtidos.

5.1 Ambiente de Execução

Experimentos foram conduzidos em ambiente operacional Linux Ubuntu 22.04 LTS, Processador Intel i7 2.7 GHz e 16GB de memória RAM. Comparamos o *DPNetTraffic* e *DPNetTraffic + PostProcessing* com três concorrentes existentes na literatura: Mecanismo Geométrico (GHOSH *et al.*, 2009), Mecanismo Log-Laplace (NY; PAPPAS, 2013) e Privbayes (ZHANG *et al.*, 2017). Tanto a abordagem proposta neste trabalho e seus concorrentes foram implementados na linguagem de programação Python, versão 3.10.0 e podem ser encontrados no GitHub[1]. Adicionalmente, os experimentos foram executados 50 vezes e a média destes resultados foram reportadas.

5.2 Conjunto de Dados

Utilizamos quatro conjuntos de dados reais: o primeiro é um conjunto de dados privado coletado em um laboratório de pesquisa localizado no Brasil, denominado *"Local Laboratory Traffic Flow"*[2]. Esse conjunto de dados possui 33.845 fluxos de rede. O segundo conjunto de dados foi coletado para fins de segurança cibernética da Universidade de New Brunswick - Canadá, denominado *"Canadian Institute for CyberSecurity"*[3]. Esse conjunto possui 140.733 fluxos de rede. Informações estatísticas sobre os dois conjuntos de dados são descritos na Tabela 3. O terceiro e quarto conjuntos de dados são usualmente adotados na literatura para fins científicos, denominados de *"Labeled Network Traffic flows"*[4] e *"IP Network*

[1] https://github.com/felpsmonteiro/masters-degree-research
[2] https://github.com/felpsmonteiro/masters-degree-research/blob/main/Datasets/traffic_table.csv
[3] https://www.unb.ca/cic/datasets/darknet2020.html
[4] https://www.kaggle.com/datasets/jsrojas/ip-network-traffic-flows-labeled-with-87-apps

Traffic Flows Labeled"[5]. Os conjuntos possuem respectivamente, 1.046.017 e 2.704.841 fluxos de rede. Informações estatísticas sobre esses dois conjuntos de dados são descritos na Tabela 4.

	Local Laboratory Traffic Flow			***Canadian Institute for CyberSecurity***		
	Portas	**Protocolos**	**Serviços**	**Portas**	**Protocolos**	**Serviços**
Contagem	29	2	25	12.794	2	30
Média	1.167,06	16.922	1.353	10	70.365	4.691
Desvio Padrão	4.281,42	15.726	4.608	342	19.736	10.326
Min	1	5.802	1	1	56.410	13
25%	2	-	2	1	-	229
50%	20	-	20	1	-	1.127
75%	140	-	140	3	-	4.201
Max	22.844	28.043	22.844	30.416	84.321	48.300

Tabela 3 – Tabela atributos estatísticos conjuntos de dados: ***Local Laboratory Traffic Flow*** **e Canadian Institute for CyberSecurity**.

	Labeled Network Traffic Flows			***IP Network Traffic Flows Labeled***		
	Portas	**Protocolos**	**Serviços**	**Portas**	**Protocolos**	**Serviços**
Contagem	8.465	2	120	33.753	2	141
Média	123	523.007	8.716	80	1.348.668	19.183
Desvio Padrão	6.165	112.761	29.832	7.638	226.192	69.599
Min	1	443.273	1	1	1.188.726	1
25%	1	-	21	1	-	18
50%	1	-	241	3	-	425
75%	2	-	2.406	5	-	5.106
Max	423.039	602.742	230.847	1.039.599	1.508.610	569.828

Tabela 4 – Tabela atributos estatísticos conjuntos de dados: ***Labeled Network Traffic Flows*** **e IP Network Traffic Flows Labeled**.

5.3 Avaliação do Ruído Introduzido

Neste trabalho, realizamos uma análise abrangente de diversas métricas e características relacionadas ao desempenho das técnicas e conjuntos de dados investigados. Além de avaliar o desempenho geral, focamos em métricas específicas, que nos permitem entender melhor o comportamento e as capacidades das técnicas em estudo ao introduzir ruído estatístico aos dados.

Uma das métricas avaliadas foi o erro relativo médio – MRE. Essa medida nos fornece informações sobre a precisão das técnicas em relação aos valores reais e ruidosos. Calculamos o erro relativo médio juntamente com um intervalo de confiança de 95% para cada

[5] https://www.kaggle.com/datasets/jsrojas/labeled-network-traffic-flows-114-applications

técnica e conjunto de dados, permitindo uma comparação direta entre elas. Essa análise nos permite identificar quais técnicas apresentam uma maior ou menor tendência a produzir ruídos significativos, fornecendo informações valiosas sobre a confiabilidade e a acurácia de cada abordagem.

Além disso, examinamos os top-*ks* serviços e portas mais frequentes. Ao determinar os principais serviços e portas mais frequentes, podemos entender melhor as áreas de especialização de cada técnica. Essa informação é especialmente relevante para a seleção da técnica mais adequada para diferentes tipos de análise e detecção de padrões em conjuntos de dados específicos.

Por fim, também consideramos o tempo de processamento como uma métrica importante. Avaliamos o tempo necessário para executar cada técnica em todos os quatro conjuntos de dados, levando em consideração a escalabilidade e a eficiência computacional de cada abordagem, ou seja, a capacidade de uma técnica se adaptar e funcionar eficientemente em cenários de grande escala, lidando com um grande volume de dados. Essa análise nos permite identificar as técnicas que são mais rápidas e eficientes em termos de tempo de processamento, o que é crucial para a aplicabilidade prática das técnicas em ambientes de grande volume de dados ou com requisitos de tempo real.

5.3.1 Erro Relativo Médio - MRE

O MRE é calculado comparando os valores originais dos dados com os valores ruidosos obtidos após a aplicação do Mecanismo de Privacidade Diferencial. Quanto menor for o valor do MRE, maior será a precisão do mecanismo na preservação da utilidade dos dados.

Normalmente, o MRE é definido como a média dos valores absolutos das diferenças relativas entre os dados originais e os dados ruidosos, divididos pelo valor absoluto dos dados originais. A fórmula geral para o cálculo do MRE é a seguinte:

$$\boldsymbol{MRE}(y,\hat{y}) = \frac{1}{N}\sum_{i=0}^{N-1}\frac{|y_i - \hat{y}_i|}{|y_i|} \tag{5.1}$$

Onde:

- N é o número total de registros no conjunto de dados;
- y_i é o valor original do registro i no conjunto de dados;

– $\hat{y}_i$ é o valor ruidoso do registro i obtido após a aplicação do Mecanismo de Privacidade Diferencial.

O MRE é uma métrica importante para avaliar a eficácia de mecanismos de Privacidade Diferencial, pois nos permite quantificar a qualidade da preservação da utilidade dos dados após a introdução de ruído. É fundamental buscar um equilíbrio entre privacidade e utilidade, garantindo que a inserção de ruído não comprometa significativamente a precisão e a confiabilidade dos resultados obtidos a partir dos dados ruidosos.

Coletamos o erro das contagens de portas, protocolos e serviços com três valores diferentes de orçamentos de privacidade ε: $0,1$, $0,5$ e $1,0$. Como mencionado na Seção 2.3.1, estes valores de orçamento de privacidade ε são comumente reportados na literatura, independente da aplicação. Os resultados de MRE com seus respectivos intervalos de confiança 95% para a média de 50 execuções são reportados na Figura 12 para o *"Local Laboratory Traffic Flow"*, Figura 13 para o *"Canadian Institute for CyberSecurity"*, Figura 14 para o *"Labeled Network Traffic flows"* e Figura 15 para o *"IP Network Traffic Flows Labeled"*.

5.3.1.1 Teste de Hipótese (t-teste e p-valor)

Realizamos também o teste de hipótese para a contagem de protocolos no conjunto de dados *"Local Laboratory Traffic Flow"*. Neste experimento, a diferença do MRE para as abordagens *DPNetTraffic + PostProcessing* e a aplicação direta da Privacidade Diferencial através do Mecanismo Geométrico são ligeiramente próximas considerando seus intervalos de confiança de 95% – Figura 12b.

Com o objetivo de determinar se os valores deste experimento são estatisticamente significantes ou não, calculamos o *p-valor* das amostras através do *t-teste*. O *t-teste* é um teste amplamente utilizado na estatística para comparar as médias de duas amostras e determinar se existem diferenças significativas entre elas. Em testes de hipóteses as duas proposições utilizadas são a hipótese nula H_0 e a hipótese alternativa H_1 (ROSS; WILLSON, 2017).

A hipótese nula H_0 é uma afirmação que assume que não há diferença estatística significativa entre duas amostras. Por exemplo, na anonimização das contagens do tráfego de rede, a hipótese nula seria que o processo de anonimização não causa alterações significativas nas respostas ruidosas em comparação com uma outra amostra. Já a hipótese alternativa H_1 é a afirmação oposta à hipótese nula. Ela assume que existe uma diferença significativa entre duas amostras. Continuando com o exemplo da anonimização do tráfego de rede, a hipótese

alternativa seria que o processo de anonimização causa alterações significativas nas respostas ruidosas em comparação com outra amostra.

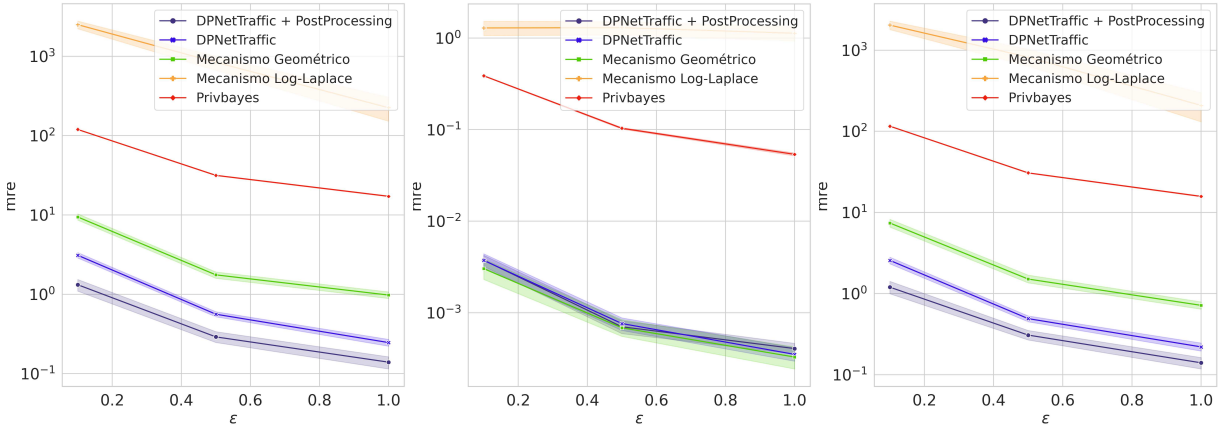
Estas hipóteses são formuladas com base no que se pretende investigar ou provar estatisticamente e são aceitas ou rejeitas de acordo com o limite pré-determinado chamado de *nível de significância*. Neste trabalho, fixamos o nível de significância em $0,05$ (NEEL; ROTH, 2018; WANG *et al.*, 2018). Logo, se o *p-valor* for maior que o nível de significância pré-definido, aceita-se a hipótese nula H_0 e consequentemente conclui-se que não há diferença significativa entre as médias das amostras.

5.3.1.2 Resultados

Conforme esperado, à medida que o orçamento de privacidade ε aumenta, o erro relativo médio diminui. Nota-se que o *DPNetTraffic* + PostProcessing apresenta melhores resultados quando comparado à aplicação direta da Privacidade Diferencial via Mecanismo Geométrico, ao mecanismo Log-Laplace e ao PrivBayes para as contagens de portas e serviços. Isto ocorre devido nossa abordagem economizar orçamento de privacidade ε em todo o processo, não necessitando de divisão.

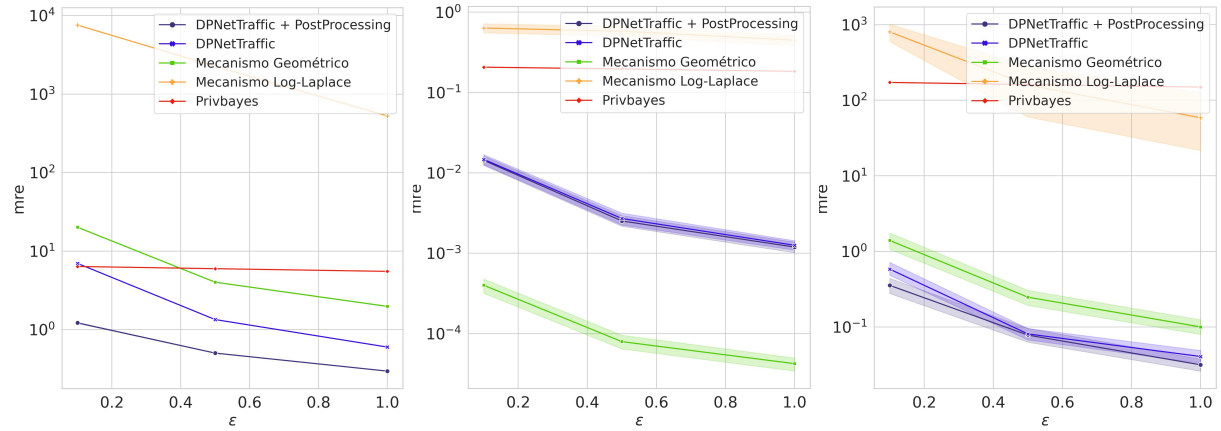
Em particular, na Figura 12 quando $\varepsilon = 0,5$, os valores do *DPNetTraffic* + PostProcessing para contagem de portas, serviços e protocolos são respectivamente $\pm 0,29$, $\pm 0,30$ e $\pm 0,0007$. Levando-se em consideração apenas o *DPNetTraffic*, isto é, sem o ajuste das contagens negativas, notam-se os valores $\pm 0,56$, $\pm 0,49$ e $\pm 0,00076$ respectivamente para portas, serviços e protocolos. Comparando-se a aplicação direta da Privacidade Diferencial através do Mecanismo Geométrico, obtêm-se respectivamente os valores: $\pm 1,75$, $\pm 1,50$ e $\pm 0,00068$. Na aplicação do mecanismo Log-Laplace, os valores do erro relativo médio são: ± 839, $\pm 1,29$ e ± 820. Considerando a aplicação do Privbayes, os valores são: ± 31, $\pm 0,1$ e ± 30. Para a contagem de protocolos (Figura 12b), nossa abordagem apresenta resultados um pouco inferiores à aplicação direta do Mecanismo Geométrico. Apesar disso, o erro médio relativo introduzido é bem baixo, isto é, na ordem de $\pm 10^{-3}$ quando $\varepsilon = 0,5$, por exemplo. Vale ressaltar que existem apenas dois protocolos (TCP e UDP) compartilhados juntamente com suas respectivas contagens.

Realizamos o teste de hipótese para a contagem de protocolos – Figura 12b – com o objetivo de investigar se há diferença estatística significativa entre as duas abordagens – *DPNetTraffic + PostProcessing* e *Mecanismo Geométrico*. Os *p-valores* correspondentes às técnicas de Privacidade Diferencial são apresentados na Tabela 5.



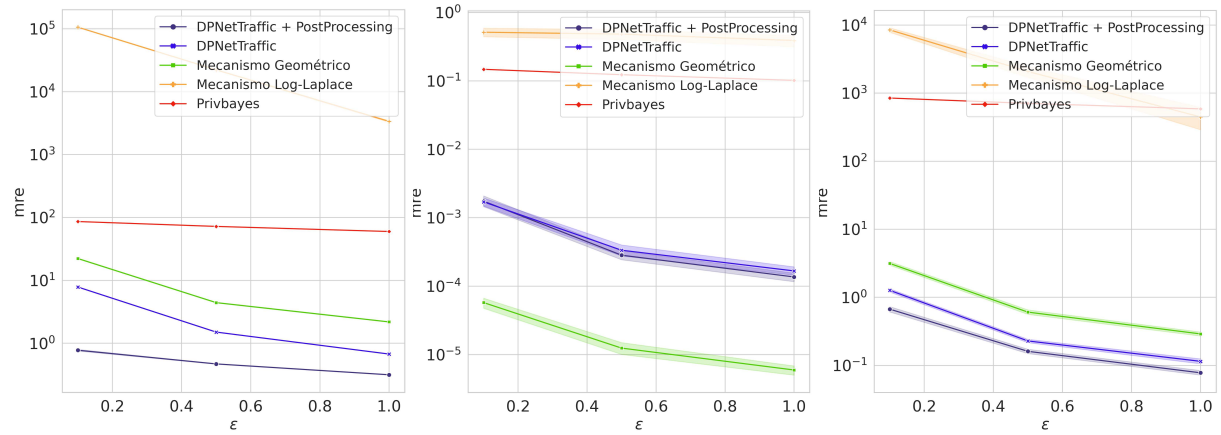
(a) Portas (b) Protocolos (c) Serviços

Figura 12 – Erro Relativo Médio do conjunto de dados: ***Local Laboratory Traffic Flow***.



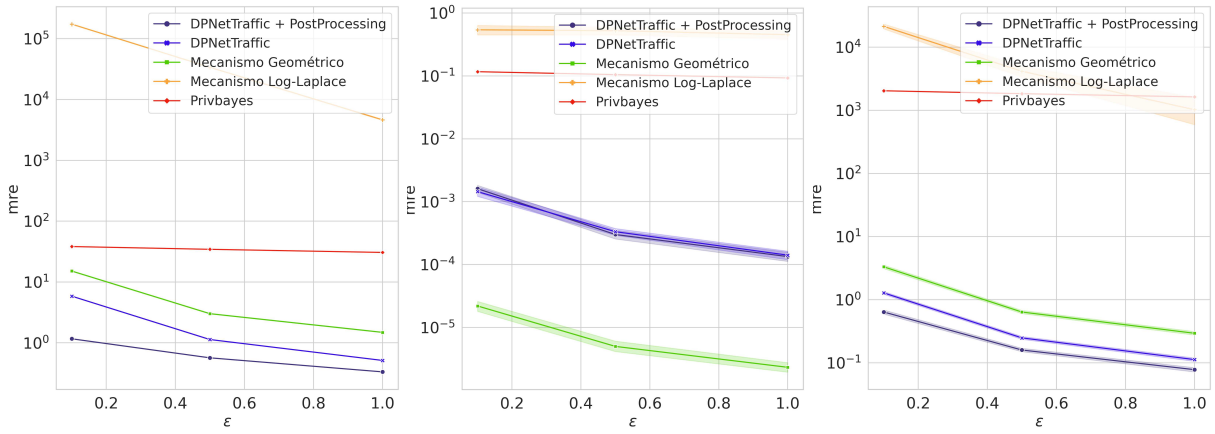
(a) Portas (b) Protocolos (c) Serviços

Figura 13 – Erro Relativo Médio do conjunto de dados: ***Canadian Institute for CyberSecurity***.



(a) Portas (b) Protocolos (c) Serviços

Figura 14 – Erro Relativo Médio do conjunto de dados: ***Labeled Network Traffic Flows***.



(a) Portas (b) Protocolos (c) Serviços

Figura 15 – Erro Relativo Médio do conjunto de dados: ***IP Network Traffic Flows Labeled***.

Abordagem	$\varepsilon = 0,1$	$\varepsilon = 0,5$	$\varepsilon = 1$
Mecanismo Geométrico	0,122	0,852	0,152
Mecanismo Log-Laplace	1,46e-19	4,52e-19	1,01e-19
Privbayes	1,76e-148	1,65e-99	1,41e-74

Tabela 5 – Tabela *p-valor – DPNetTraffic + PostProcessing* e concorrentes para o conjunto de dados: Local Laboratory Traffic Flow - Figura 12b Protocolos.

Observamos que o *p-valor* para a contagem de protocolos – Figura 12b, quando o $\varepsilon = 0,5$ é de $0,852$. De acordo com o nível de significância estabelecido em $0,05$, não há evidências estatísticas suficientes para rejeitar a hipótese nula. O mesmo comportamento ocorre para os demais orçamentos de privacidade na Figura 12b, isto é, quando o $\varepsilon = 0,1$ e $\varepsilon = 1$.

Em outras palavras, não há fundamentos para afirmar que existe uma diferença significativa ou um efeito entre as amostras anonimizadas. O *p-valor* de $0,122$, $0,852$ e $0,125$, respectivamente para $\varepsilon = 0,1$, $\varepsilon = 0,5$ e $\varepsilon = 1$, são maiores que o nível de significância estabelecido de $0,05$, indicando que os resultados observados podem ser explicados pela variação aleatória dos dados, e não por um efeito real ou significativo.

Os resultados no segundo conjunto de dados, *"Canadian Institure For CyberSecurity"* – Figura 13, apresentam um comportamento similar. Especificamente, quando $\varepsilon = 0,5$, os valores da nossa abordagem *DPNetTraffic* + PostProcessing para contagem de portas, protocolos e serviços são respectivamente $\pm 0,502$, $\pm 0,0025$ e $\pm 0,078$. Já para o *DPNetTraffic*, nossa abordagem sem o ajuste das contagens negativas, observam-se os valores $\pm 1,34$, $\pm 0,0027$ e $\pm 0,081$ respectivamente para portas, protocolos e serviços. Quando comparamos com a

aplicação direta da Privacidade Diferencial, obtêm-se respectivamente, quando o $\varepsilon = 0,5$, valores $\pm 4,01$, $\pm 0,00007$ e $\pm 0,248$. Na aplicação do mecanismo Log-Laplace, os valores do erro relativo médio são: ± 2258, $\pm 0,579$ e ± 159. Considerando a aplicação do Privbayes, os valores são: $\pm 5,96$, $\pm 0,196$ e ± 161.

Os resultados no terceiro conjunto de dados, *"Labeled Network Traffic Flows"* – Figura 14, indicam um comportamento semelhante assim como os outros conjuntos de dados mencionados anteriormente. Em particular, quando o $\varepsilon = 0,5$, os valores obtidos pela nossa abordagem *DPNetTraffic* + *PostProcessing* para a contagem de portas e serviços são, $\pm 0,469$ e $\pm 0,16$. Já para o *DPNetTraffic*, observam-se os respectivos valores para contagem de portas e serviços: $\pm 1,50$ e $\pm 0,228$. Os valores $\pm 4,42$ e $\pm 0,606$ são obtidos considerando a aplicação do Mecanismo Geométrico para o mesmo conjunto de dados.

Por fim, no quarto conjunto de dados *'IP Network Traffic Flows Labeled"*, considerando o mesmo valor de ε e a nossa abordagem *DPNetTraffic* + *PostProcessing*, as contagens para portas, protocolos e serviços são respectivamente: $\pm 0,567$, $\pm 0,003$ e $\pm 0,159$. Na aplicação do *DPNetTraffic*, os respectivos valores para portas, protocolos e serviços são: $\pm 1,13$, $\pm 0,0033$ e $\pm 0,248$, isto é, não considerando o ajuste das contagens negativas. Quando comparamos com a aplicação do Mecanismo Geométrico obtemos: $\pm 3,015$, $\pm 0,000005$ e $\pm 0,637$ respectivamente para portas, protocolos e serviços.

A contagem de protocolos para Figura 13b, 14b, 15b utilizando a abordagem proposta também apresenta resultados moderadamente superiores quando comparada ao mecanismo Geométrico. Novamente, mesmo com esses resultados, o erro médio relativo introduzido é bem baixo, isto é, na ordem de $\pm 10^{-3}$ quando $\varepsilon = 0,5$, por exemplo.

5.3.2 Avaliação dos Top-k Serviços e Portas

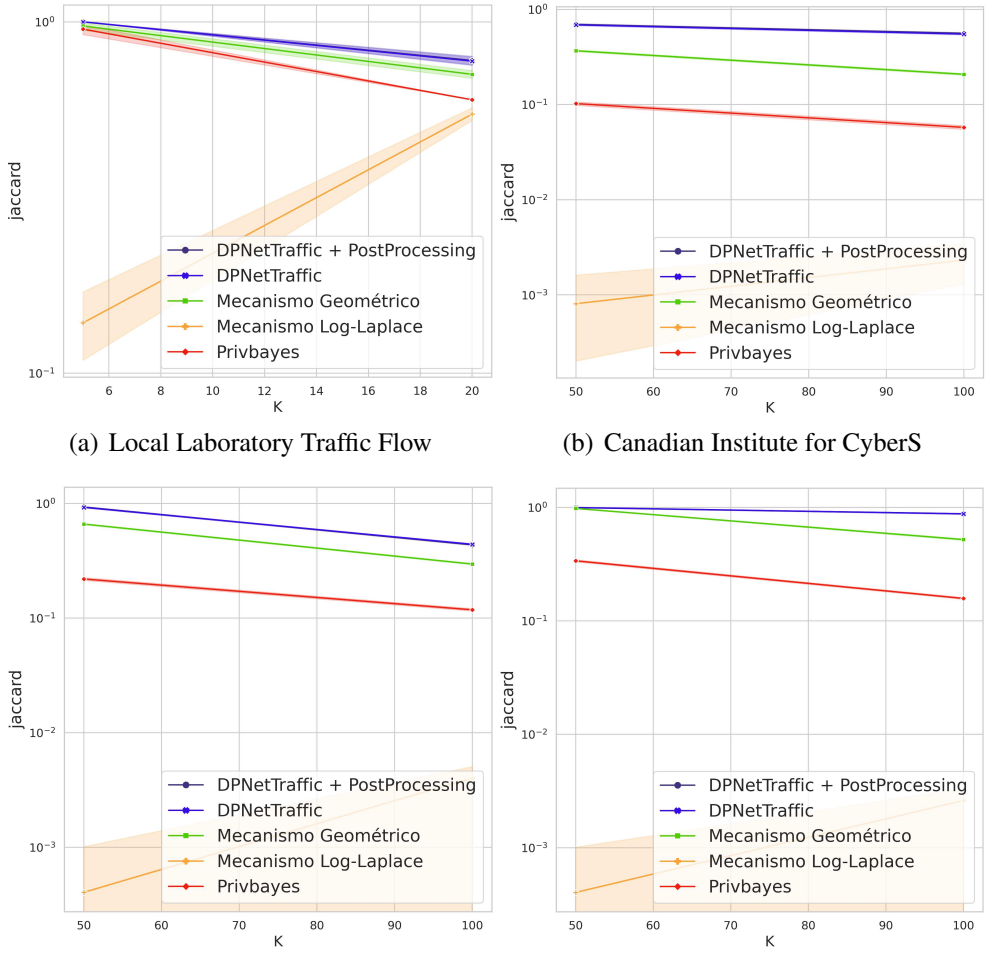
Contagens diferencialmente privadas podem ser utilizadas também para identificar os serviços ou portas mais frequentes, medindo os top-*ks* registros mais utilizados em ambos os conjuntos de dados e avaliando a similaridade de Jaccard.

Esses resultados são exibidos nas Figuras 16 e 17. Convém salientar que, para protocolos, os resultados referentes a top-*ks* não são reportados, visto que ambos os conjuntos de dados possuem apenas 2 tipos de protocolos: TCP e UDP. A similaridade de Jaccard é dada pela seguinte fórmula:

$$Jaccard(y,\hat{y}) = \frac{|y \cap \hat{y}|}{|y \cup \hat{y}|} \tag{5.2}$$

onde y e $\hat{y}$ são os conjuntos de top-k original e ruidoso, respectivamente. Valores próximos de 1 sugerem que os dois conjuntos são muito similares, enquanto que valores próximos de 0 indicam que os conjuntos y e $\hat{y}$ são mais disjuntos. Nos resultados obtidos, estabelecemos um orçamento de privacidade ε de $0,1$. Escolhemos esse valor específico, pois representa o menor ε avaliado, o que proporciona um nível mais elevado de privacidade aos dados. Além disso, variamos os valores de *ks* para explorar diferentes configurações e analisar seu impacto nos resultados.

Nota-se que tanto o *DPNetTraffic*, quanto o *DPNetTraffic + PostProcessing* apresentam um desempenho notavelmente superior em comparação a outras técnicas e mecanismos diferencialmente privados, quando analisados os aspectos de Jaccard e top-k. Essas métricas são cruciais para avaliar a utilidade dos dados preservada durante o processo de rivacidade Diferencial.



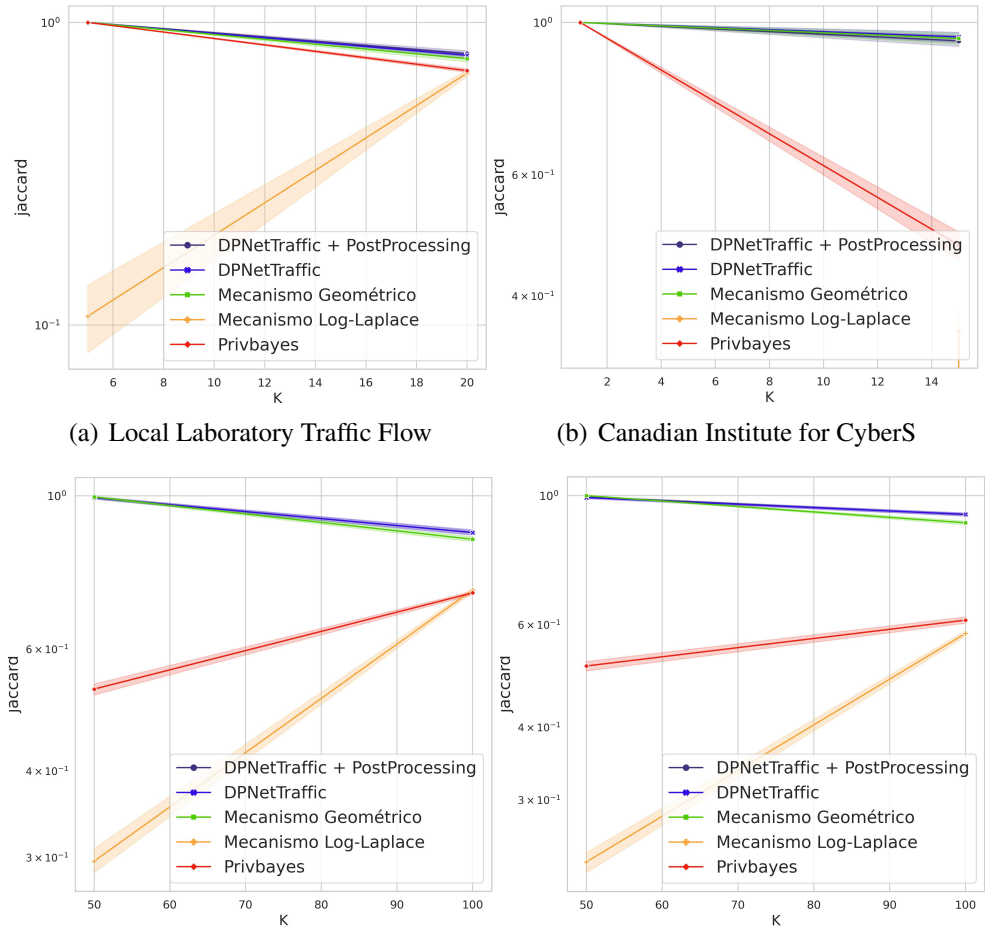
(a) Local Laboratory Traffic Flow

(b) Canadian Institute for CyberS

(c) Labeled Network Traffic Flows

(d) IP Network Traffic Flows Lab

Figura 16 – Similaridade de Jaccard para contagem de portas.



(a) Local Laboratory Traffic Flow

(b) Canadian Institute for CyberS

(c) Labeled Network Traffic Flows

(d) IP Network Traffic Flows Lab

Figura 17 – Similaridade de Jaccard para contagem de portas.

Ao considerar a similaridade de Jaccard, que mede a similaridade entre dois conjuntos, nossa abordagem mostrou-se mais eficiente em preservar a utilidade dos dados. Isso significa que os resultados obtidos pela nossa abordagem são mais próximos dos resultados que seriam obtidos se não houvesse a aplicação da Privacidade Diferencial. Além disso, ao considerar a avaliação dos top-*ks* serviços e portas, nossa abordagem mostrou-se especialmente eficaz em preservar as informações mais relevantes.

Os top-*ks* representam os principais elementos de interesse nos conjuntos de dados, e garantir sua preservação é fundamental para não comprometer a utilidade dos resultados finais. Nossa abordagem demonstrou uma maior capacidade de manter a qualidade e a relevância desses elementos, assegurando que a análise realizada permaneça confiável e precisa. Portanto, podemos afirmar que a abordagem proposta neste trabalho é promissora em termos de Privacidade Diferencial, oferecendo um equilíbrio adequado entre a proteção dos dados sensíveis e a preservação da utilidade dos resultados.

5.3.3 Tempo de Processamento

A avaliação do tempo de processamento de algoritmos é uma tarefa essencial para compreender o desempenho e a eficiência de sistemas computacionais. A Privacidade Diferencial é uma técnica fundamental para proteger a privacidade dos dados durante o processamento de informações sensíveis. Uma preocupação comum ao utilizar essa abordagem é o impacto no tempo de processamento. No entanto, é importante ressaltar que o tempo de execução de algoritmos que incorporam a Privacidade Diferencial não é necessariamente custoso.

A medição do tempo de processamento de algoritmos pode ser realizada por meio da análise empírica ou teórica. A análise empírica envolve a execução do algoritmo em um ambiente controlado, registrando o tempo de execução e repetindo o processo várias vezes para obter uma média confiável. Já a análise teórica baseia-se em modelos matemáticos e análise de complexidade algorítmica para prever o tempo de processamento com base em características do algoritmo, como o tamanho da entrada e o número de operações realizadas. Para fins de referência, neste trabalho, realizamos a análise de forma empírica, registrando o tempo de execução em 50 iterações e calculando a média dos resultados.

Vale também ressaltar que o tempo de processamento também depende do tamanho e complexidade dos dados, bem como dos parâmetros escolhidos para a Privacidade Diferencial, como o valor de ε. Um menor ε pode introduzir um nível mais alto de ruído nos resultados, o que pode aumentar o tempo de processamento. No entanto, é possível encontrar um equilíbrio entre a precisão dos resultados e o tempo de execução, ajustando os parâmetros de acordo com as necessidades específicas do problema. Graças aos avanços tecnológicos e ao desenvolvimento de algoritmos eficientes, muitas implementações da Privacidade Diferencial podem ser executadas de forma rápida e eficaz. Na Figura 18, é possível analisar o tempo de execução das técnicas que atendem à Privacidade Diferencial em conjunto de dados reais.

Analisando os resultados para o conjunto de dados *Local Laboratory Traffic Flow*, em particular quando o $\varepsilon = 0,5$, observa-se que as abordagens *DPNetTraffic + PostProcessing*, *DPNetTraffic*, Mecanismo Geométrico e Mecanismo Log-Laplace apresentam tempos médios de processamento muito próximos. Respectivamente os valores para cada abordagem são: $0,0523$s, $0,0526$s, $0,0511$s, $0,0511$s.

No entanto, a abordagem Privbayes se destaca por apresentar um tempo médio de processamento significativamente maior para o mesmo conjunto de dados e o mesmo ε, com um valor de $1,195$s. Isso indica que essa abordagem é computacionalmente mais custosa

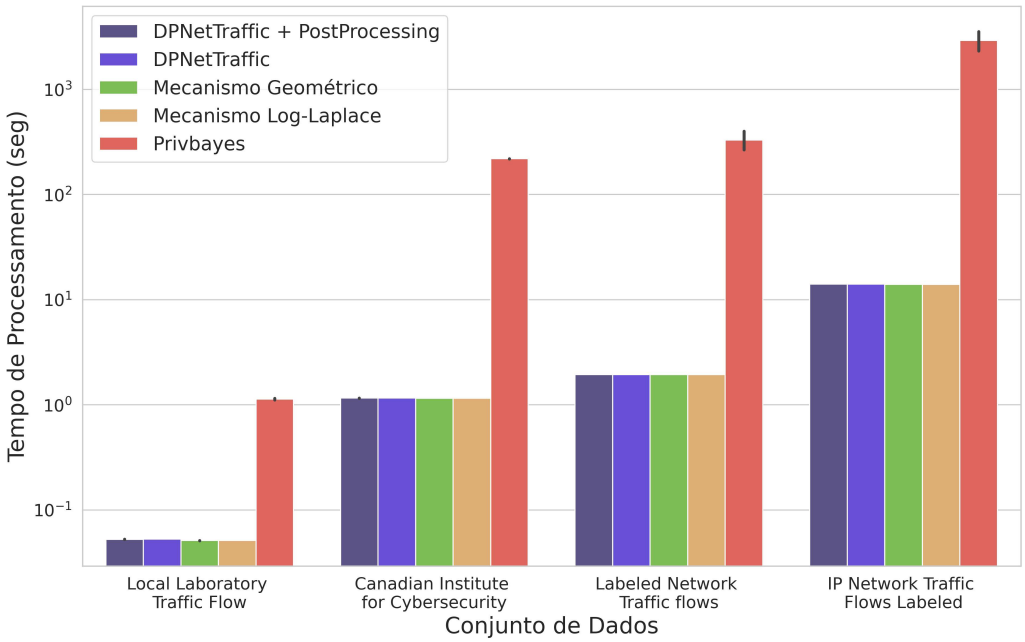


Figura 18 – Tempo de Processamento de Execução das técnicas de Privacidade Diferencial $\varepsilon = 0,5$.

em comparação com as outras técnicas avaliadas. Esse aumento significativo no tempo de processamento pode ser atribuído à complexidade computacional envolvida na aplicação do algoritmo Privbayes.

Para o conjunto de dados do *Canadian Institute for Cybersecurity* com um valor de $\varepsilon = 0,5$, as abordagens analisadas apresentaram um comportamento semelhante ao conjunto de dados discutido anteriormente. Os tempos de execução registrados foram de $1,16$s, $1,157$s, $1,153$s e $1,153$s, respectivamente, para as abordagens *DPNetTraffic + PostProcessing*, *DPNetTraffic*, Mecanismo Geométrico e Mecanismo Log-Laplace. No entanto, foi observado que o Privbayes teve um tempo de execução significativamente maior de 219s. Essa diferença novamente pode ser atribuída a uma maior complexidade computacional associada ao algoritmo Privbayes em comparação com as outras abordagens utilizadas neste conjunto de dados.

No caso do conjunto de dados *Labeled Network Traffic flows*, os valores de tempo de execução das abordagens são os seguintes: $1,938$ segundos para a abordagem *DPNetTraffic + PostProcessing*, $1,94$ segundos para *DPNetTraffic*, $1,936$ segundos para o Mecanismo Geométrico, $1,936$ segundos para o Mecanismo Log-Laplace e $46,9$ segundos para o Privbayes.

Para o último conjunto de dados, *IP Network Traffic Flows Labeled*, os tempos de execução das abordagens são: $14,014$ segundos para *DPNetTraffic + PostProcessing*, $14,022$ segundos para *DPNetTraffic*, $14,006$ segundos para o Mecanismo Geométrico, $14,004$ segundos

para o Mecanismo Log-Laplace e $155,95$ segundos para o Privbayes.

Observa-se que em todos os conjuntos de dados analisados, o Privbayes apresentou um tempo de execução significativamente maior em comparação com as outras abordagens. Conforme discutido na Seção 2.3.5.4, o Privbayes utiliza uma abordagem baseada em aprendizado de redes Bayesianas para a geração de dados sintéticos diferencialmente privados. Esse processo envolve a construção de uma estrutura de rede Bayesiana e a inferência dos parâmetros da rede, o que pode exigir um tempo computacionalmente mais intenso em comparação com outros métodos de geração de dados sintéticos.

A abordagem *DPNetTraffic + PostProcessing* demonstrou um desempenho satisfatório em relação à escalabilidade dos conjuntos de dados. Conforme os conjuntos de dados aumentaram em tamanho, os tempos de execução da abordagem *DPNetTraffic + PostProcessing* se mantiveram relativamente estáveis. Isso indica que a abordagem é capaz de lidar eficientemente com conjuntos de dados maiores sem comprometer significativamente o tempo de execução. Essa escalabilidade é um fator importante a ser considerado ao lidar com conjuntos de dados em expansão, pois garante que a abordagem possa ser aplicada de forma eficiente em cenários com um número crescente de registros.

Além disso, a abordagem *DPNetTraffic + PostProcessing* destaca-se ao combinar a eficácia do mecanismo *DPNetTraffic* com um processo adicional de pós-processamento, cujo objetivo é aprimorar a utilidade dos dados gerados por meio do ajuste de contagens negativas. Essa estratégia possibilita alcançar um equilíbrio ideal entre a preservação da privacidade e a maximização da utilidade dos dados, proporcionando uma solução abrangente e robusta para o desafio de garantir a privacidade dos indivíduos.

Em resumo, o tempo de processamento de algoritmos que incorporam Privacidade Diferencial não precisa ser excessivamente custoso. Com técnicas adequadas, implementações eficientes e ajuste dos parâmetros, é possível obter resultados precisos e proteger a privacidade dos dados sem comprometer significativamente o tempo de execução. Isso permite que a Privacidade Diferencial seja uma solução viável e acessível para garantir a confidencialidade das informações em diversas aplicações. A abordagem *DPNetTraffic + PostProcessing* mostra-se promissora em termos de escalabilidade, fornecendo uma solução eficiente e eficaz em conjuntos de dados em crescimento. Isso permite que os pesquisadores e profissionais de privacidade de dados trabalhem com conjuntos de dados cada vez maiores, mantendo a privacidade dos indivíduos e preservando a utilidade dos dados para análises e tomada de decisões.

5.4 Conclusão

Este trabalho apresentou uma abordagem eficaz para aplicar a Privacidade Diferencial na publicação de 3 informações importantes no tráfego de redes, contagem de portas, protocolos e serviços. Os resultados obtidos demonstraram a capacidade da abordagem em reduzir os erros relativos médios, preservar a utilidade dos dados e manter a confiabilidade das análises realizadas. Além disso, o tempo de processamento necessário para executar o algoritmo foi razoável, evidenciando a viabilidade, escalabilidade e eficiência da nossa abordagem em cenários práticos. Esses resultados promissores reforçam a relevância do *DPNetTraffic + PostProcessing* como uma solução confiável e computacionalmente eficiente para proteger a privacidade dos usuários.

6 CONCLUSÃO E TRABALHOS FUTUROS

Neste capítulo, apresentamos um resumo dos resultados desta dissertação e fornecemos orientações para trabalhos futuros.

6.1 Resumo dos Resultados

Neste trabalho, propusemos uma abordagem diferencialmente privada denominada *DPNetTraffic*, que busca garantir a privacidade de dados de tráfego de rede e estar em conformidade com as leis de privacidade existentes, como a Lei Geral de Proteção de Dados (LGPD), o Regulamento Geral de Proteção de Dados (GDPR) e as diretrizes da Comissão Federal de Comunicações (FCC). Essas leis e regulamentos têm como objetivo proteger a privacidade dos indivíduos e impor regras para o tratamento de dados pessoais.

Com o objetivo de garantir a privacidade dos usuários, diversas técnicas foram propostas nas últimas décadas. Por exemplo, o *k-anonimity* e seus derivados, tais como *l-diversity*, δ*-presence* e *t-closeness*. No entanto, essas abordagens pressupõem que um adversário possui conhecimento limitado, o que não é verdade em situações do mundo real.

O *DPNetTraffic* é uma solução inovadora que visa atender aos requisitos legais de privacidade, ao mesmo tempo em que permite a utilização e análise dos dados de tráfego de rede de forma útil e segura. No *pipeline* de anonimização do *DPNetTraffic*, inicialmente agrupamos os dados em triplas contendo portas, protocolos e serviços, para que a adição de ruído fosse executada apenas uma vez, ao invés de três vezes utilizando a abordagem mais usual de Privacidade Diferencial. Em seguida, o mecanismo Geométrico foi aplicado sobre as contagens de cada tripla pré-processada, a fim de introduzir ruído aleatório na contagem original. Por fim, obtemos as contagens agregadas por portas de destino, protocolos e serviços via pós-processamento de dados, isto é, o objetivo final da nossa abordagem. Propomos também uma técnica para lidar com as contagens negativas produzidas pelos mecanismos diferencialmente privados, uma vez que eles seguem e adicionam ruídos aos dados a partir de uma distribuição.

Através da avaliação dos erros relativos médios, foi possível observar que nossa abordagem se destacou ao preservar a integridade dos dados e minimizar as distorções introduzidas pelo processo de Privacidade Diferencial. Os valores dos erros relativos médios foram bastante baixos, de pelo menos 35%, indicando que os resultados obtidos pela nossa abordagem se aproximaram de maneira satisfatória dos resultados reais que seriam obtidos sem a aplicação

da Privacidade Diferencial.

Com base no último estágio do nosso *pipeline* de anonimização, isto é, nossa proposta para lidar com as contagens negativas, realizamos aprimoramentos no *DPNetTraffic*, resultando no *DPNetTraffic + PostProcessing*, que apresentou um desempenho superior ao adicionar menos ruído aos dados anonimizados. Observou-se em média uma redução de até $57,4\%$ no ruído adicionado às contagens de portas, $26,55\%$ nas contagens de serviços e até $9,93\%$ nas contagens de protocolos, em comparação com *DPNetTraffic*.

Esses resultados indicam uma melhoria significativa na preservação da utilidade dos dados anonimizados, com uma redução proporcional no nível de distorção introduzido pelo mecanismo de Privacidade Diferencial. O processo de pós-processamento aplicado ao *DPNetTraffic* permitiu um refinamento dos dados anonimizados, resultando em uma maior acurácia das contagens de portas, serviços e protocolos. Essa abordagem demonstrou ser eficaz em equilibrar a privacidade dos dados com a qualidade e utilidade das informações resultantes.

Além disso, a análise dos top-k serviços e portas também evidenciou a eficácia da nossa abordagem. Ao preservar as informações mais relevantes e garantir sua qualidade, nossa abordagem mostrou-se capaz de manter a utilidade dos resultados finais, mesmo após a aplicação da Privacidade Diferencial. Isso é essencial para garantir que as análises realizadas com base nessas informações continuem sendo confiáveis e úteis para a tomada de decisões.

Quanto ao tempo de processamento, nossa abordagem demonstrou ser uma solução viável, escalável e eficiente. O tempo necessário para executar o algoritmo foi razoável e semelhante aos concorrentes, o que significa que a aplicação da Privacidade Diferencial não implica em um custo computacional excessivo. Isso é uma vantagem significativa, pois permite a aplicação prática da Privacidade Diferencial em cenários reais, sem comprometer a eficiência e a escalabilidade do processo.

Dessa forma, os resultados obtidos neste trabalho são promissores e indicam que a abordagem proposta pode ser uma solução eficaz para preservar a privacidade dos dados sensíveis enquanto mantém a utilidade dos resultados. Com a crescente preocupação com a privacidade e a segurança dos dados, a aplicação da Privacidade Diferencial torna-se cada vez mais relevante. Nossa abordagem contribui para esse campo, oferecendo uma solução confiável, precisa e computacionalmente eficiente para a análise de serviços e portas em conjuntos de dados sensíveis.

6.2 Trabalhos Futuros

Como trabalhos futuros espera-se investigar informações privadas em outros domínios de redes, tais como duração do fluxo de tráfego, tamanho do fluxo e comprimento do fluxo de rede. Para isso, será necessário desenvolver técnicas específicas de privacidade diferencial para lidar com esses tipos de dados, não apenas com contagens. Além disso, pretende-se estudar a aplicação da abordagem *DPNetTraffic* em ambientes que envolvam a geração e o processamento contínuo de dados em tempo real. Para essa finalidade, planeja-se adotar a Privacidade Diferencial Local (PDL), a qual insere ruído diretamente nos pontos de geração de dados, antes mesmo de serem compartilhados ou processados.

REFERÊNCIAS

ABOWD, J.; ASHMEAD, R.; CUMINGS-MENON, R.; GARFINKEL, S.; KIFER, D.; LECLERC, P.; SEXTON, W.; SIMPSON, A.; TASK, C.; ZHURAVLEV, P. An uncertainty principle is a price of privacy-preserving microdata. **Advances in neural information processing systems**, v. 34, p. 11883–11895, 2021.

AGRAWAL, A.; VERSCHUEREN, R.; DIAMOND, S.; BOYD, S. A rewriting system for convex optimization problems. **Journal of Control and Decision**, Taylor & Francis, v. 5, n. 1, p. 42–60, 2018.

ALANI, M. M.; ALANI, M. M. Tcp/ip model. **Guide to OSI and TCP/IP models**, Springer, p. 19–50, 2014.

BREWSTER, T. **Now Those Privacy Rules Are Gone, This Is How ISPs Will Actually Sell Your Personal Data**. 2017. Https://www.forbes.com/sites/thomasbrewster/2017/03/30/fcc-privacy-rules-how-isps-will-actually-sell-your-data/?sh=23565f2d21d1. Acesso em: 15 de abril de 2023.

BRITO, F. T.; MACHADO, J. C. Preservação de privacidade de dados: Fundamentos, técnicas e aplicações. **Jornadas de atualização em informática**, p. 91–130, 2017.

BUREAU, U. C. **Census Bureau sets key parameters to protect privacy in 2020 census results**. 2021. https://www.census.gov/newsroom/press-releases/2021/2020-census-key-parameters.html. Acesso em: 03 de fevereiro de 2023.

CASSOLA, A.; BLASS, E.-O.; NOUBIR, G. Authenticating privately over public wi-fi hotspots. In: **Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security**. [*S. l.*: *s. n.*], 2015. p. 1346–1357.

Comissão Federal de Comunicação. **Privacidade do cliente**. 2018. https://www.fcc.gov/general/customer-privacy. Acesso em: 17 de fevereiro de 2023.

COTTON, M.; EGGERT, L.; TOUCH, D. J. D.; WESTERLUND, M.; CHESHIRE, S. **Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry**. RFC Editor, 2023. RFC 6335. (Request for Comments, 6335). Disponível em: https://www.rfc-editor.org/info/rfc6335.

CRESWELL, A.; WHITE, T.; DUMOULIN, V.; ARULKUMARAN, K.; SENGUPTA, B.; BHARATH, A. A. Generative adversarial networks: An overview. **IEEE signal processing magazine**, IEEE, v. 35, n. 1, p. 53–65, 2018.

DHARMAWAN, N. K. S.; KASIH, D. P. D.; STIAWAN, D. Personal data protection and liability of internet service provider: a comparative approach. **International Journal of Electrical and Computer Engineering (IJECE)**, v. 9, n. 4, p. 3175–3184, 2019.

DWORK, C. Differential privacy. In: SPRINGER. **International Colloquium on Automata, Languages, and Programming**. [*S. l.*], 2006. p. 1–12.

DWORK, C. Differential privacy: A survey of results. In: SPRINGER. **Theory and Applications of Models of Computation: 5th International Conference, TAMC 2008, Xi'an, China, April 25-29, 2008. Proceedings 5**. [*S. l.*], 2008. p. 1–19.

DWORK, C.; KOHLI, N.; MULLIGAN, D. Differential privacy in practice: Expose your epsilons! **Journal of Privacy and Confidentiality**, v. 9, n. 2, 2019.

DWORK, C.; MCSHERRY, F.; NISSIM, K.; SMITH, A. Calibrating noise to sensitivity in private data analysis. In: SPRINGER. **Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006. Proceedings 3**. [*S. l.*], 2006. p. 265–284.

DWORK, C.; ROTH, A. *et al.* The algorithmic foundations of differential privacy. **Foundations and Trends® in Theoretical Computer Science**, Now Publishers, Inc., v. 9, n. 3–4, p. 211–407, 2014.

FARIAS, V. A.; BRITO, F. T.; FLYNN, C.; MACHADO, J. C.; MAJUMDAR, S.; SRIVASTAVA, D. Local dampening: Differential privacy for non-numeric queries via local sensitivity. **The VLDB Journal**, Springer, p. 1–24, 2023.

FURNO, A.; FIORE, M.; STANICA, R. Joint spatial and temporal classification of mobile traffic demands. In: IEEE. **IEEE INFOCOM 2017-IEEE Conference on Computer Communications**. [*S. l.*], 2017. p. 1–9.

GANEV, G.; OPRISANU, B.; CRISTOFARO, E. D. Robin hood and matthew effects: Differential privacy has disparate impact on synthetic data. In: PMLR. **International Conference on Machine Learning**. [*S. l.*], 2022. p. 6944–6959.

GARCÍA-DORADO, J. L.; FINAMORE, A.; MELLIA, M.; MEO, M.; MUNAFO, M. Characterization of isp traffic: Trends, user habits, and access technology impact. **IEEE Transactions on Network and Service Management**, IEEE, v. 9, n. 2, p. 142–155, 2012.

GDPR. **General Data Protection Regulation**. 2018. https://gdpr-info.eu/. Acesso em: 17 de fevereiro de 2023.

GHOSH, A.; ROUGHGARDEN, T.; SUNDARARAJAN, M. Universally utility-maximizing privacy mechanisms. In: **Proceedings of the forty-first annual ACM symposium on Theory of computing**. [*S. l.*: *s. n.*], 2009. p. 351–360.

HINTZE, K.; GRAHAM, S.; DUNLAP, S.; SWEENEY, P. Infiniband network monitoring: Challenges and possibilities. In: SPRINGER. **Critical Infrastructure Protection XV: 15th IFIP WG 11.10 International Conference, ICCIP 2021, Virtual Event, March 15–16, 2021, Revised Selected Papers 15**. [*S. l.*], 2022. p. 187–208.

HOOFF, J. V. D.; LAZAR, D.; ZAHARIA, M.; ZELDOVICH, N. Vuvuzela: Scalable private messaging resistant to traffic analysis. In: **Proceedings of the 25th Symposium on Operating Systems Principles**. [*S. l.*: *s. n.*], 2015. p. 137–152.

IANA. **Internet Assigned Numbers Authority**. 2023. https://www.iana.org/. Acesso em: 24 de março de 2023.

JORDON, J.; YOON, J.; SCHAAR, M. V. D. Pate-gan: Generating synthetic data with differential privacy guarantees. In: **International conference on learning representations**. [*S. l.*: *s. n.*], 2019.

JOSHI, M.; HADI, T. H. A review of network traffic analysis and prediction techniques. **arXiv preprint arXiv:1507.05722**, 2015.

KUROSE, J. F.; ROSS, K. W.; ZUCCHI, W. L. **Redes de Computadores ea Internet: uma abordagem top-down**. [*S. l.*]: Pearson Addison Wesley, 2013.

LGPD. **Lei Geral de Proteção de Dados Pessoais**. 2019. http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 17 de fevereiro de 2023.

LI, C.; HAY, M.; RASTOGI, V.; MIKLAU, G.; MCGREGOR, A. Optimizing linear counting queries under differential privacy. In: **Proceedings of the twenty-ninth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems**. [*S. l.*: *s. n.*], 2010. p. 123–134.

LI, N.; LI, T.; VENKATASUBRAMANIAN, S. Closeness: A new privacy measure for data publishing. **IEEE Transactions on Knowledge and Data Engineering**, IEEE, v. 22, n. 7, p. 943–956, 2009.

LU, Y.; TIAN, H.; SHEN, H.; XU, D. Privacy preserving classification based on perturbation for network traffic. In: SPRINGER. **Parallel and Distributed Computing, Applications and Technologies: 19th International Conference, PDCAT 2018, Jeju Island, South Korea, August 20-22, 2018, Revised Selected Papers 19**. [*S. l.*], 2018. p. 121–132.

MACHANAVAJJHALA, A.; HE, X.; HAY, M. Differential privacy in the wild: A tutorial on current practices & open challenges. In: **Proceedings of the 2017 ACM International Conference on Management of Data**. [*S. l.*: *s. n.*], 2017. p. 1727–1730.

MACHANAVAJJHALA, A.; KIFER, D.; GEHRKE, J.; VENKITASUBRAMANIAM, M. l-diversity: Privacy beyond k-anonymity. **ACM Transactions on Knowledge Discovery from Data (TKDD)**, ACM New York, NY, USA, v. 1, n. 1, p. 3–es, 2007.

MCSHERRY, F. D. Privacy integrated queries: an extensible platform for privacy-preserving data analysis. In: **Proceedings of the 2009 ACM SIGMOD International Conference on Management of data**. [*S. l.*: *s. n.*], 2009. p. 19–30.

MIRIMIR. **Collection of User Data by ISPs and Telecom Providers, and Sharing with Third Parties**. 2018. Https://www.ivpn.net/blog/collection-of-user-data-by-isps-and-telecom-providers-and-sharing-with-third-parties. Acesso em: 28 de março de 2023.

NDATINYA, V.; XIAO, Z.; MANEPALLI, V. R.; MENG, K.; XIAO, Y. Network forensics analysis using wireshark. **International Journal of Security and Networks**, Inderscience Publishers (IEL), v. 10, n. 2, p. 91–106, 2015.

NEAR, J. P.; ABUAH, C. **Programming Differential Privacy**. [*S. n.*], 2021. v. 1. Disponível em: https://uvm-plaid.github.io/programming-dp/.

NEEL, S.; ROTH, A. Mitigating bias in adaptive data gathering via differential privacy. In: PMLR. **International Conference on Machine Learning**. [*S. l.*], 2018. p. 3720–3729.

NERGIZ, M. E. *et al.* Hiding the presence of individuals from shared databases. In: **Proceedings of the 2007 ACM SIGMOD international conference on Management of data**. [*S. l.*: *s. n.*], 2007. p. 665–676.

NISSIM, K.; RASKHODNIKOVA, S.; SMITH, A. Smooth sensitivity and sampling in private data analysis. In: **Proceedings of the thirty-ninth annual ACM symposium on Theory of computing**. [*S. l.*: *s. n.*], 2007. p. 75–84.

NY, J. L.; PAPPAS, G. J. Privacy-preserving release of aggregate dynamic models. In: **Proceedings of the 2nd ACM international conference on High confidence networked systems**. [*S. l.*: *s. n.*], 2013. p. 49–56.

PARENTONI, L. N. Responsabilidade civil dos provedores de serviços na internet: Breves notas. **Âmbito Jurídico**, 2009.

PATIL, A.; SINGH, S. Differential private random forest. In: IEEE. **2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI)**. [*S. l.*], 2014. p. 2623–2630.

PETERSON, L. L.; DAVIE, B. S. **Computer networks: a systems approach**. [*S. l.*]: Elsevier, 2007.

ROSS, A.; WILLSON, V. L. Independent samples t-test. In: **Basic and advanced statistical tests**. [*S. l.*]: Brill, 2017. p. 13–16.

SANGEETHA, S.; SADASIVAM, G. S. Privacy of big data: a review. **Handbook of big data and iot security**, Springer, p. 5–23, 2019.

SHAFIQ, M.; YU, X.; LAGHARI, A. A.; YAO, L.; KARN, N. K.; ABDESSAMIA, F. Network traffic classification techniques and comparative analysis using machine learning algorithms. In: IEEE. **2016 2nd IEEE International Conference on Computer and Communications (ICCC)**. [*S. l.*], 2016. p. 2451–2455.

STREIT, A. G.; LEÃO, R. M.; SOUZA, E. de; MENASCHÉ, D. S. *et al.* Descobrindo perfis de tráfego de usuários: uma abordagem nao supervisionada. In: SBC. **Anais do XXXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos**. [*S. l.*], 2019. p. 169–182.

SWEENEY, L. k-anonymity: A model for protecting privacy. **International journal of uncertainty, fuzziness and knowledge-based systems**, World Scientific, v. 10, n. 05, p. 557–570, 2002.

TANENBAUM, A. S.; WETHERALL, D. **Network Computer 6th Edition**. [*S. l.*]: Pearson, 2021.

ULLMAN, J. **What is Synthetic Data?** 2022. https://differentialprivacy.org/synth-data-0/. Acesso em: 05 de junho de 2023.

VIDAL, I. de C.; MENDONÇA, A. L. da C.; ROUSSEAU, F.; MACHADO, J. de C. Protecting: An application of local differential privacy for iot at the edge in smart home scenarios. In: SBC. **Anais do XXXVIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos**. [*S. l.*], 2020. p. 547–560.

WANG, Y.; KIFER, D.; LEE, J. Differentially private confidence intervals for empirical risk minimization. **arXiv preprint arXiv:1804.03794**, 2018.

WEIL, J.; KUARSINGH, V.; DONLEY, C.; LILJENSTOLPE, C.; AZINGER, M. **IANA-Reserved IPv4 Prefix for Shared Address Space**. RFC Editor, 2012. RFC 6598. (Request for Comments, 6598). Disponível em: https://www.rfc-editor.org/info/rfc6598.

WOLTERS, P. The security of personal data under the gdpr: a harmonized duty or a shared responsibility? **International Data Privacy Law**, Oxford University Press, v. 7, n. 3, p. 165–178, 2017.

YANG, Y.; ZHANG, Z.; MIKLAU, G.; WINSLETT, M.; XIAO, X. Differential privacy in data publication and analysis. In: **Proceedings of the 2012 ACM SIGMOD International Conference on Management of Data**. [*S. l.*: *s. n.*], 2012. p. 601–606.

ZHANG, J. *et al.* Privbayes: Private data release via bayesian networks. **ACM Transactions on Database Systems (TODS)**, ACM New York, NY, USA, v. 42, n. 4, p. 1–41, 2017.

ZHANG, X.; HAMM, J.; REITER, M. K.; ZHANG, Y. Defeating traffic analysis via differential privacy: a case study on streaming traffic. **International Journal of Information Security**, Springer, v. 21, n. 3, p. 689–706, 2022.