D-NAC: Controle de acesso distribuído para redes de dados nomeados

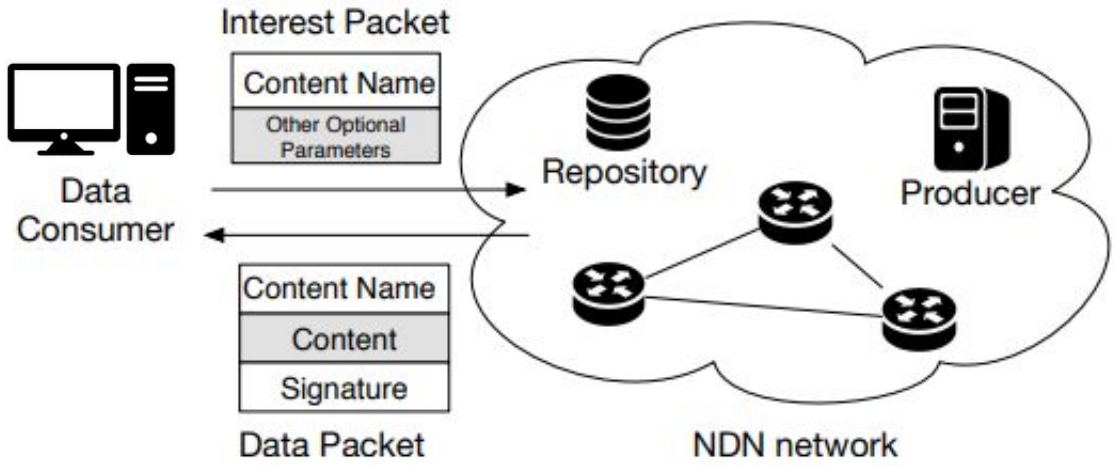
Italo Valcy S Brito
Katharine Schramm
Leobino Sampaio

Agenda

- Controle de acesso em NDN e descrição do problema
- Trabalhos relacionados
- Proposta D-NAC
- Caso de uso: ndnflix
- Avaliação experimental
- Considerações finais

Controle de Acesso em NDN (1)

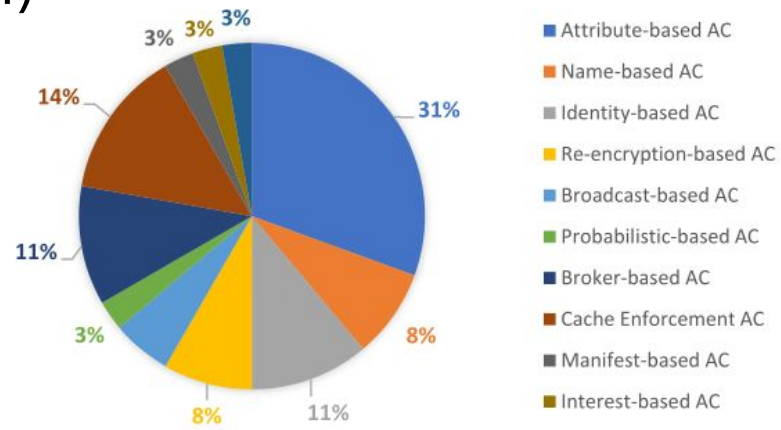
- *Named-Data Networking* (NDN): arquitetura de Internet do Futuro
  - paradigma Redes Centradas na Informação (ICN)
- Modelo de comunicação centrado nos dados *versus* entrega de pacotes centrado nos hosts
- Uso de esquema de nomeação semanticamente enriquecido para roteamento de conteúdo na rede
- Encaminhamento *stateful*
- Cache oportunístico
- Segurança dos dados
  - TCP/IP: segurança do canal



Controle de Acesso em NDN (2)

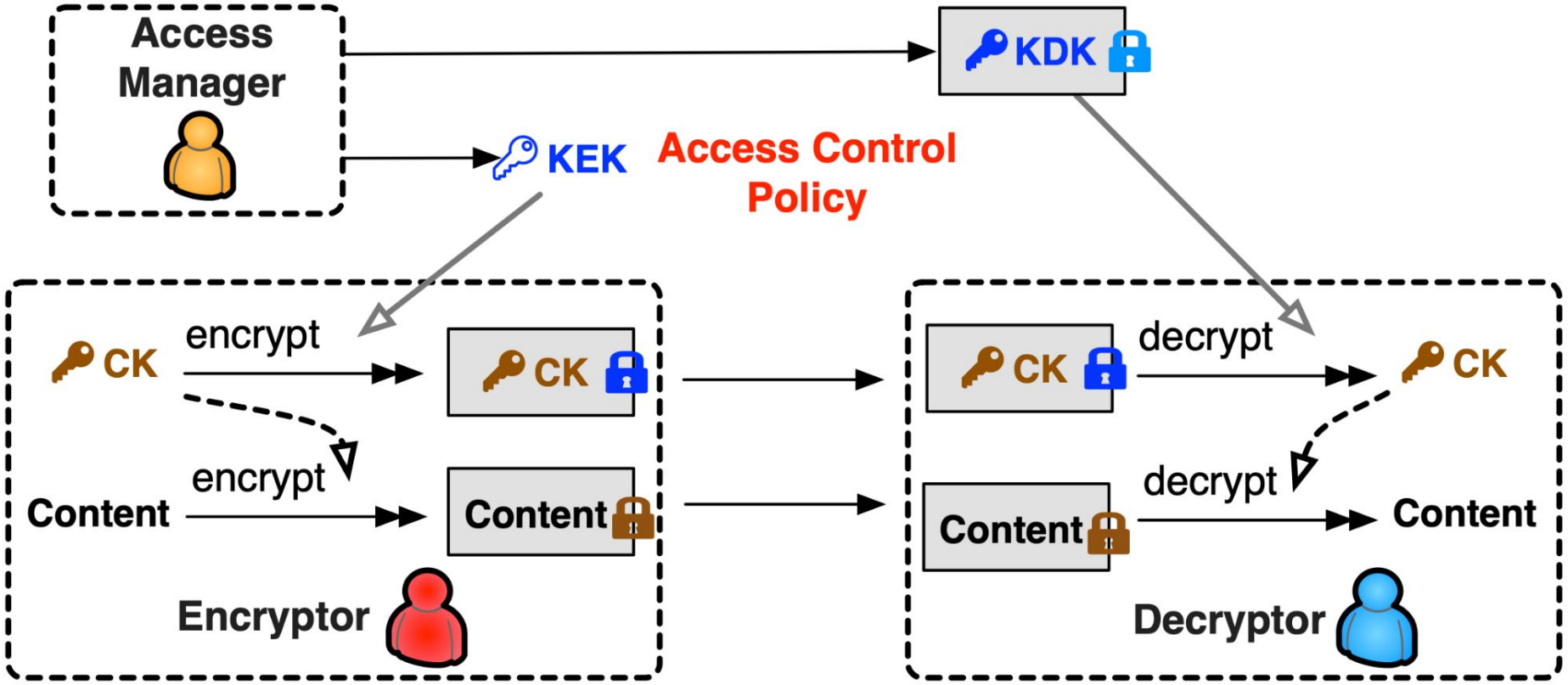
- Requisito: de acordo com o modelo de negócio, controle e contabilização de acesso com base no consumidor
  - Criptografia e gerenciamento de chaves para prover confidencialidade
  - Desafio: manutenção das características essenciais da arquitetura (foco na informação, não no consumidor/host)

- Diversos mecanismos propostos [Nour et al. 2021], com destaque para a proposta NAC de [Zhang et al. 2018]



Mecanismos de AC em NDN [Nour et al. 2021]

Controle de Acesso em NDN (3)



Descrição do problema

- Problemas do NAC: Centralização contrastante com o modelo totalmente distribuído da NDN
  - Possíveis gargalos na recuperação da KDK
  - Possível indisponibilidade do serviço

Trabalhos relacionados

- Session-based access control [Hamdane et al. 2013b]: usa dois nomes diferentes para cada conteúdo, nomes públicos e seguros. A principal desvantagem é a sobrecarga associado a várias réplicas do conteúdo disponíveis na rede.
- Access control enforcement [Wang et al. 2014]: Elimina o uso de listas de controle de acesso e usa um novo modelo criptográfico, contudo seu esquema proposto não levou em consideração mudanças dinâmicas e redes de grande escala
- Data-based access control [Hamdane et al. 2013a]: Propõe um mecanismo de controle de acesso baseado em dados com base no uso de criptografia e senha de bloqueio. Contudo, criar e gerar todas as redes para adicionar novos direitos de acesso pode se tornar um tarefa desafiante.

Proposta: D-NAC

- Descentralização dos papéis do Gerenciador de Acesso
  - Gerenciador de acesso distribuído

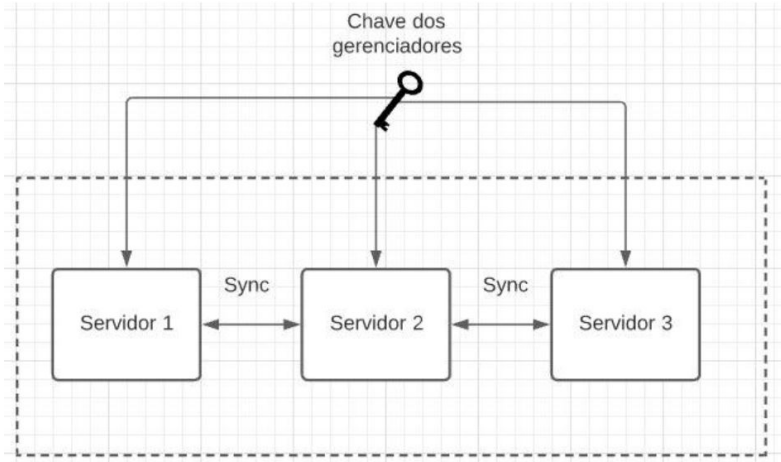
- Descoberta de serviço: Como os consumidores saberão encontrar o gerenciador de acesso mais próximo de si na rede
  - NDVR - NDN Distance Vector Routing [Brito and Sampaio 2021]
- Consistência entre gerenciadores: Como garantir a consistência de políticas de acesso entre gerenciadores
  - SVS - State Vector Sync [Moll and Zhang 2021]

Caso de uso: ndnflix

- Serviço fictício de distribuição de filmes e séries para múltiplos assinantes
- Esquema de nomeação:
  - **Produtor:**
    - Prefixo: `/ndnflix`
    - Dataset: `/ndnflix/brazil`
    - Conteúdo:
      - `/ndnflix/brazil/series/<nome da série>/<seq>`
      - `/ndnflix/brazil/filmes/<nome do filme>/<seq>`
  - **Gerenciador de acesso:**
    - Prefixo: `/ndnflix/NAC/<dataset>`
    - Chaves:
      - `/<Prefixo>/KEK/<key-id>`
      - `/<Prefixo>/KDK/<key-id>/ENCRYPTED-BY/<ChaveAssinante>`
  - **Consumidor:** `/<PrefixoProvedor>/<NomeUsuario>/KEY/<ChaveID>`

D-NAC

- Protótipo do D-NAC foi desenvolvido em C++ utilizando a biblioteca ndn-cxx
  - https://gitlab.com/katharineschramm/d-nac
- D-NAC definimos quatro classes: Manager, Consumer, Producer e Operator.
  - Necessário a definição de uma chave mestre compartilhada entre os gerenciadores de acesso



Premissas para prova de conceito

- O produtor de conteúdo conhece o prefixo do Gerenciador de Acesso;
- Existe um processo confiável de distribuição de chaves entre os gerenciadores que ocorre previamente a inicialização do D-NAC.

NAC: implementação original

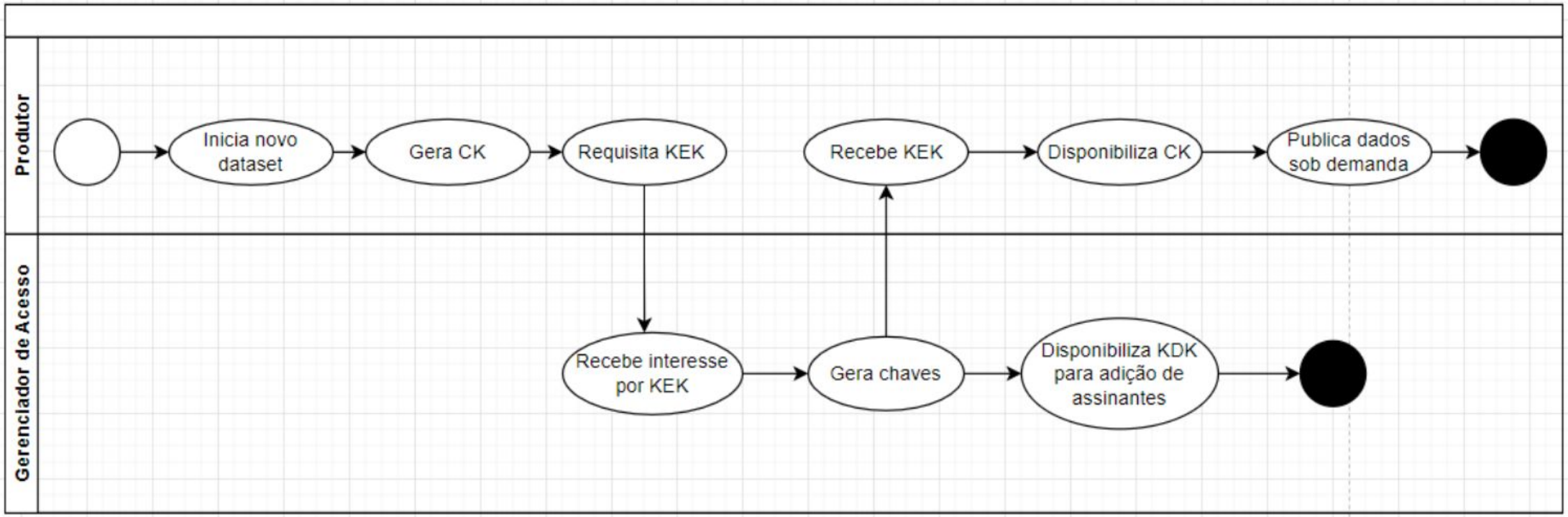


Figura 2. Fluxo de recuperação da KEK no NAC

D-NAC: modificações

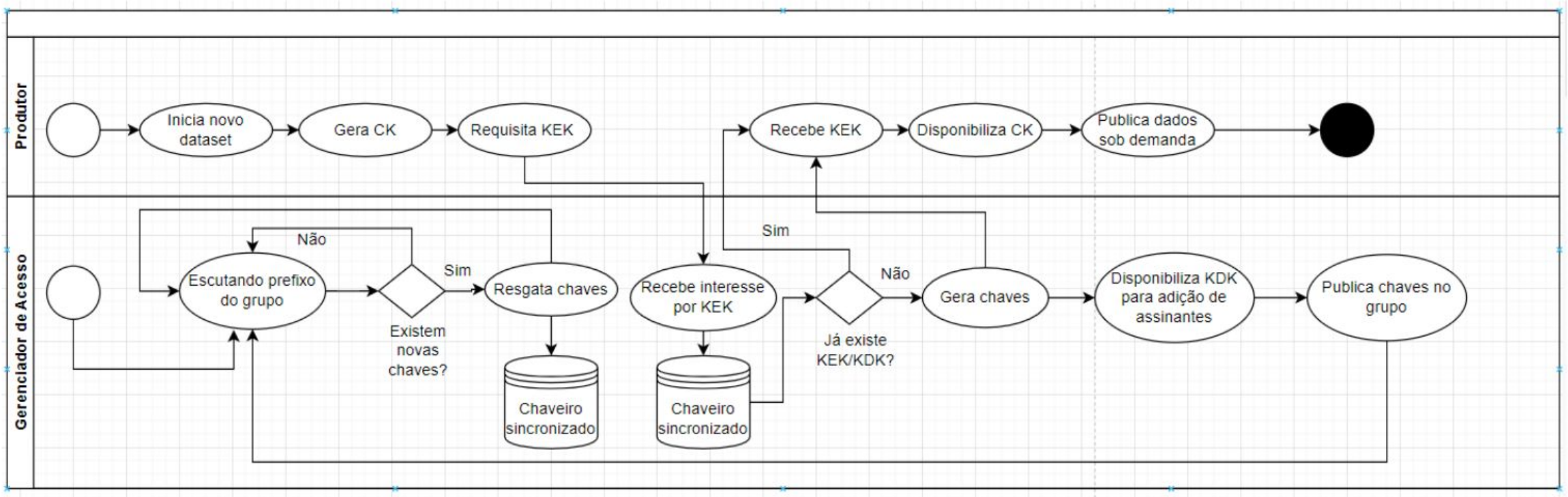


Figura 3. Fluxo de recuperação da KEK no D-NAC

D-NAC: consumidor

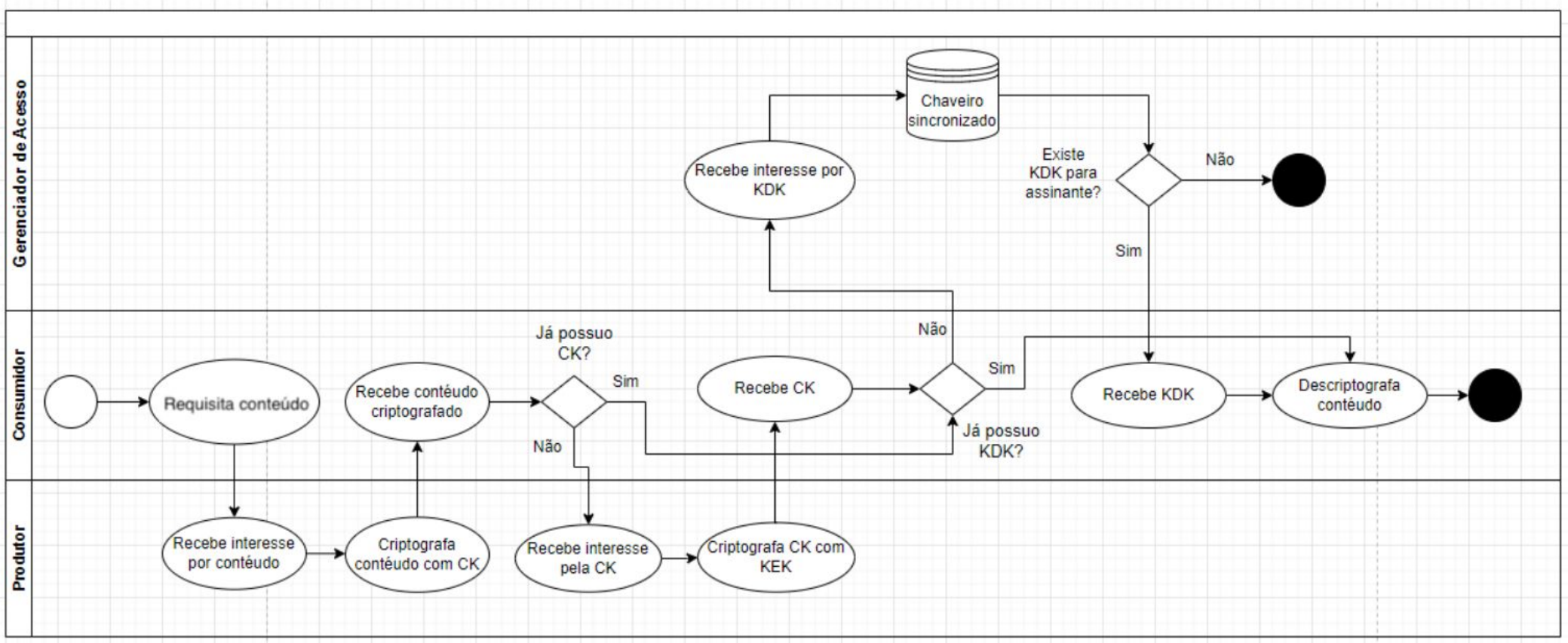
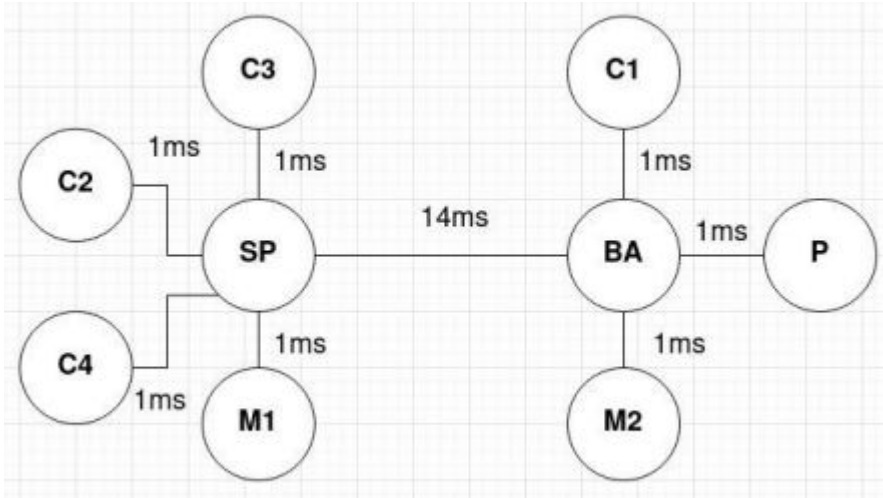


Figura 5. Fluxo de requisição da KDK no D-NAC

Avaliação experimental

- Validação de funcionamento
  - Cenário de normalidade (balanceamento de carga)
  - Cenários de falha
- Análise comparativa NAC e D-NAC
  - Atraso para recuperação dos dados
  - Sobrecarga do protocolo



Avaliação experimental

- Validação de funcionamento: Cenários de falha

```
1638282399.706403 DEBUG: [nac.AccessManager] Received interest
for key: /ndnflix/NAC/dataset/ndnflix/brazil/KDK/%EF%3D%ED%01ad
F%D2/ENCRYPTED-BY/ufba/leobino/KEY/%BA%BD%1AQr%1A_%3A
1638282399.706434 DEBUG: [nac.AccessManager] Serving /ndnflix/N
AC/dataset/ndnflix/brazil/KDK/%EF%3D%ED%01adF%D2/ENCRYPTED-BY/u
fba/leobino/KEY/%BA%BD%1AQr%1A_%3A from InMemoryStorage
1638282404.964961 DEBUG: [nac.AccessManager] Received interest
for key: /ndnflix/NAC/dataset/ndnflix/brazil/KDK/%EF%3D%ED%01ad
F%D2/ENCRYPTED-BY/usp/alice/KEY/%99x%F5%1C%10%F1%82a
1638282404.965337 DEBUG: [nac.AccessManager] Serving /ndnflix/N
AC/dataset/ndnflix/brazil/KDK/%EF%3D%ED%01adF%D2/ENCRYPTED-BY/u
sp/alice/KEY/%99x%F5%1C%10%F1%82a from InMemoryStorage
1638282409.725723 DEBUG: [nac.AccessManager] Received interest
for key: /ndnflix/NAC/dataset/ndnflix/brazil/KDK/%EF%3D%ED%01ad
F%D2/ENCRYPTED-BY/vivo/sp/pedro/KEY/%E3%88%D6%C9%93%A56%84
1638282409.725836 DEBUG: [nac.AccessManager] Serving /ndnflix/N
AC/dataset/ndnflix/brazil/KDK/%EF%3D%ED%01adF%D2/ENCRYPTED-BY/v
ivo/sp/pedro/KEY/%E3%88%D6%C9%93%A56%84 from InMemoryStorage
1638282430.110416 DEBUG: [nac.AccessManager] Received interest
for key: /ndnflix/NAC/dataset/ndnflix/brazil/KDK/%EF%3D%ED%01ad
F%D2/ENCRYPTED-BY/unesp/lucas/KEY/%FB%EA%12%1EobqB
1638282430.110562 DEBUG: [nac.AccessManager] Serving /ndnflix/N
AC/dataset/ndnflix/brazil/KDK/%EF%3D%ED%01adF%D2/ENCRYPTED-BY/u
nesp/lucas/KEY/%FB%EA%12%1EobqB from InMemoryStorage
```

Falha M2

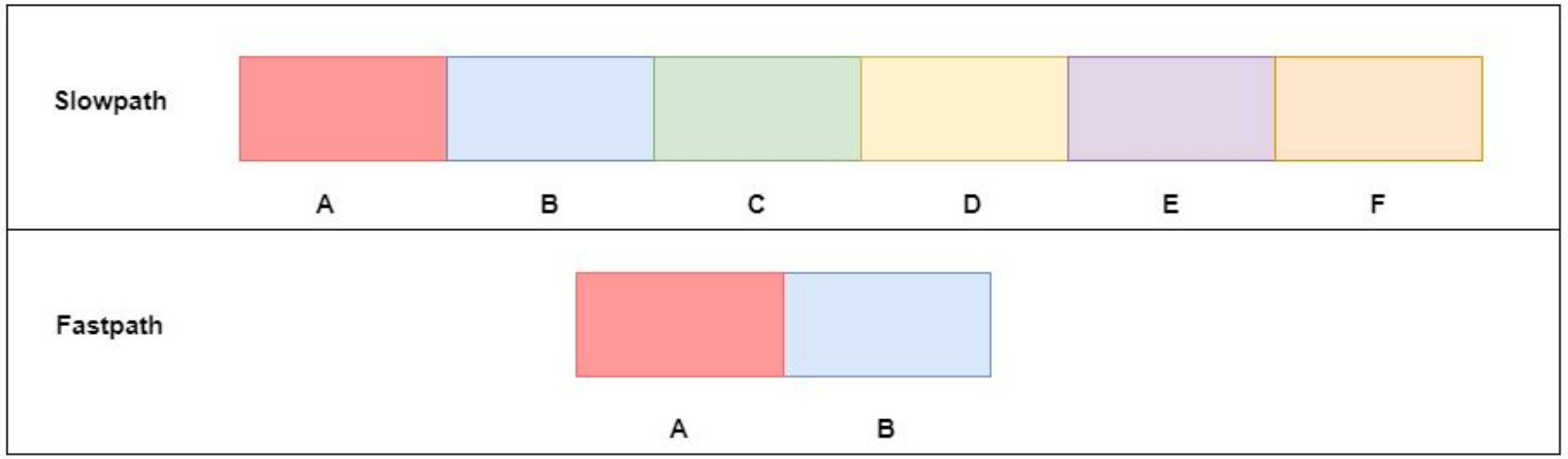
```
1638279897.064307 DEBUG: [nac.AccessManager] Received interest
for key: /ndnflix/NAC/dataset/ndnflix/brazil/KDK/%8BOX_%D1%D7%B
2%08/ENCRYPTED-BY/ufba/leobino/KEY/%CC%C0%5E%04%A64%C0N
1638279897.064348 DEBUG: [nac.AccessManager] Serving /ndnflix/N
AC/dataset/ndnflix/brazil/KDK/%8BOX_%D1%D7%B2%08/ENCRYPTED-BY/u
fba/leobino/KEY/%CC%C0%5E%04%A64%C0N from InMemoryStorage
1638279901.426945 DEBUG: [nac.AccessManager] Received interest
for key: /ndnflix/NAC/dataset/ndnflix/brazil/KDK/%8BOX_%D1%D7%B
2%08/ENCRYPTED-BY/usp/alice/KEY/%83%28%19%15%DA%D7%91%FA
1638279901.426976 DEBUG: [nac.AccessManager] Serving /ndnflix/N
AC/dataset/ndnflix/brazil/KDK/%8BOX_%D1%D7%B2%08/ENCRYPTED-BY/u
sp/alice/KEY/%83%28%19%15%DA%D7%91%FA from InMemoryStorage
1638279906.333092 DEBUG: [nac.AccessManager] Received interest
for key: /ndnflix/NAC/dataset/ndnflix/brazil/KDK/%8BOX_%D1%D7%B
2%08/ENCRYPTED-BY/vivo/sp/pedro/KEY/%99O%5D%8A%7C%E2%B7%E4
1638279906.333206 DEBUG: [nac.AccessManager] Serving /ndnflix/N
AC/dataset/ndnflix/brazil/KDK/%8BOX_%D1%D7%B2%08/ENCRYPTED-BY/v
ivo/sp/pedro/KEY/%99O%5D%8A%7C%E2%B7%E4 from InMemoryStorage
1638279926.463440 DEBUG: [nac.AccessManager] Received interest
for key: /ndnflix/NAC/dataset/ndnflix/brazil/KDK/%8BOX_%D1%D7%B
2%08/ENCRYPTED-BY/unesp/lucas/KEY/%AF%7D%DE%D9v%E1%8Fj
1638279926.463548 DEBUG: [nac.AccessManager] Serving /ndnflix/N
AC/dataset/ndnflix/brazil/KDK/%8BOX_%D1%D7%B2%08/ENCRYPTED-BY/u
nesp/lucas/KEY/%AF%7D%DE%D9v%E1%8Fj from InMemoryStorage
```

Falha M1

Avaliação experimental

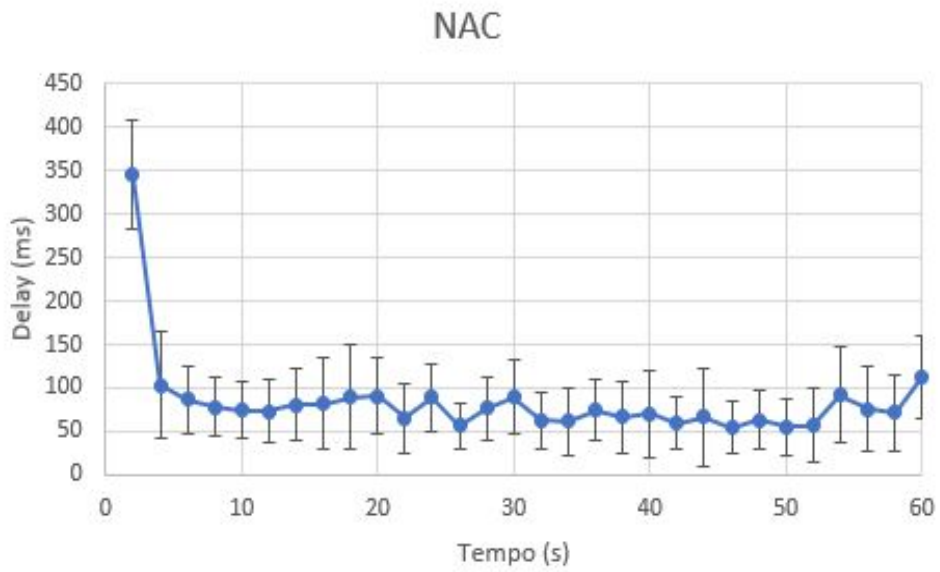
- Análise comparativa NAC e D-NAC
  - Ambiente: emulação MiniNDN, VM com 4GB RAM e 4 vCPU Intel Xeon 3.40GHz
  - Duração de 60 segundos
  - Assinantes enviam interesses para o produtor a cada 2 segundos
  - Cada teste com 10 repetições, intervalo de confiança de 95%
- Métricas
  - Atraso para recuperação dos dados (*slow path* e *fast path*)
  - Sobrecarga do protocolo

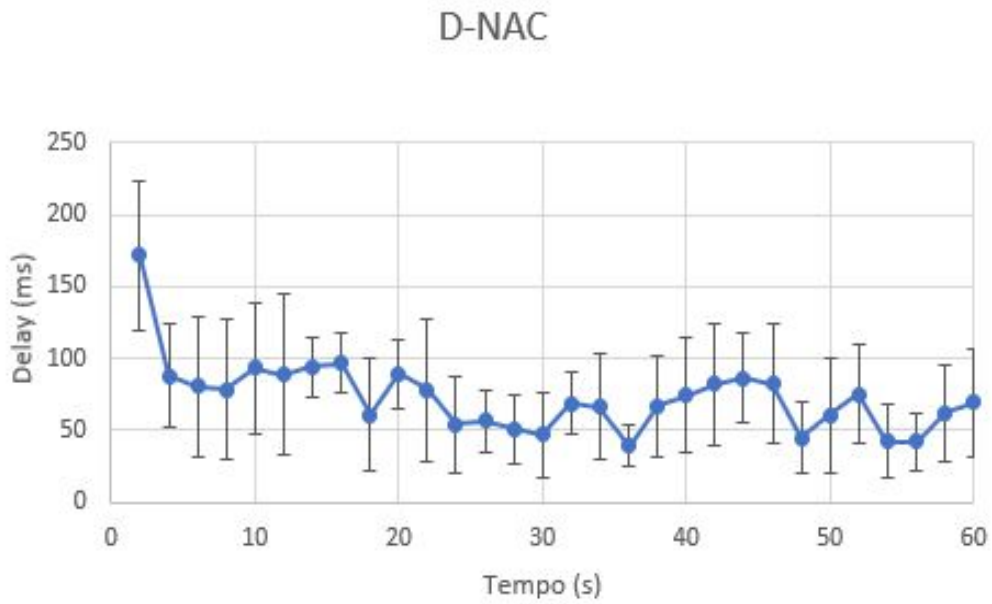
Avaliação experimental



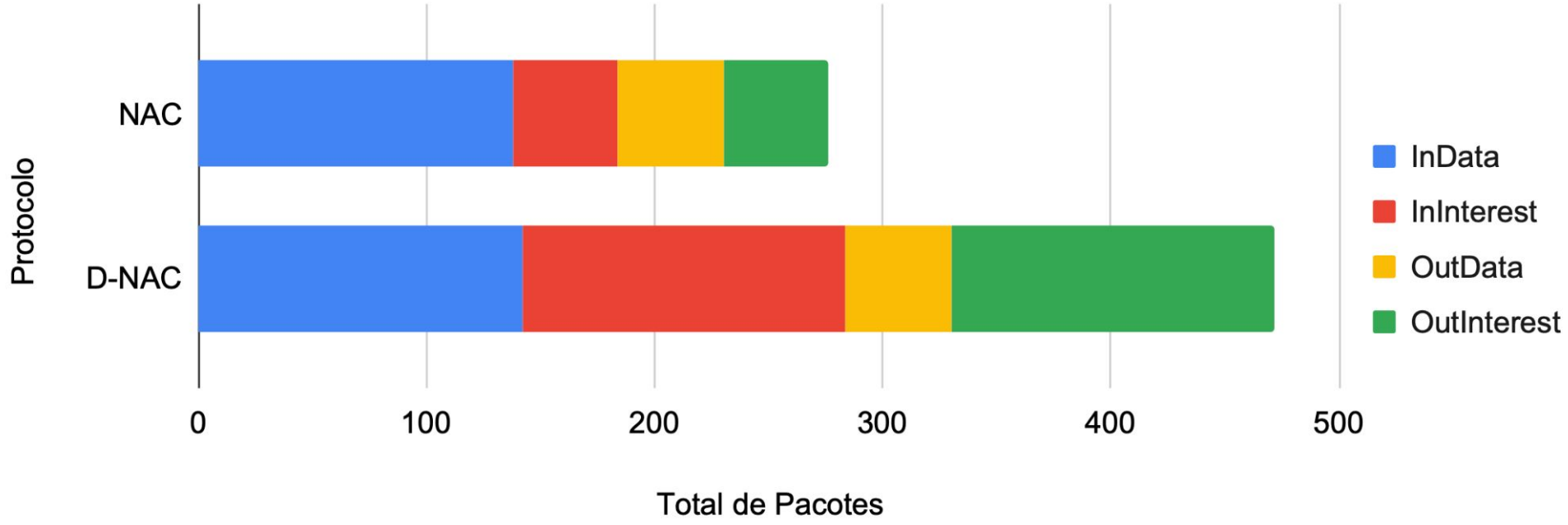
- **A**: Tempo para interesse chegar ao produtor
- **B**: Tempo para dado chegar ao assinante
- **C**: Tempo para interesse pela CK chegar ao produtor
- **D**: Tempo para CK chegar ao assinante
- **E**: Tempo para interesse da KDK chegar ao gerenciador
- **F**: Tempo para KDK chegar ao assinante

Atraso na recuperação de dados





Sobrecarga do protocolo



Considerações finais e trabalhos futuros

- Artigo apresentou o *design* e prototipagem do D-NAC, uma solução distribuída para controle de acesso em NDN
  - Inclusão de novo componente (gerenciador de acesso distribuído)
  - Customização no esquema de nomeação
  - Integração com protocolos de sincronização (SVS) e roteamento (NDVR)
- Resultados observados: melhor resiliência para falhas no gerenciador de acesso, balanceamento de carga, otimização do *slowpath* para recuperação de dados
  - Baixa sobrecarga adicional
- Trabalhos futuros:
  - Desacoplamento do design do NAC e protocolos SVS e NDVR
  - Avaliação de desempenho mais abrangente

Perguntas?

Italo Valcy da Silva Brito
e-mail: *italovalcy@ufba.br*