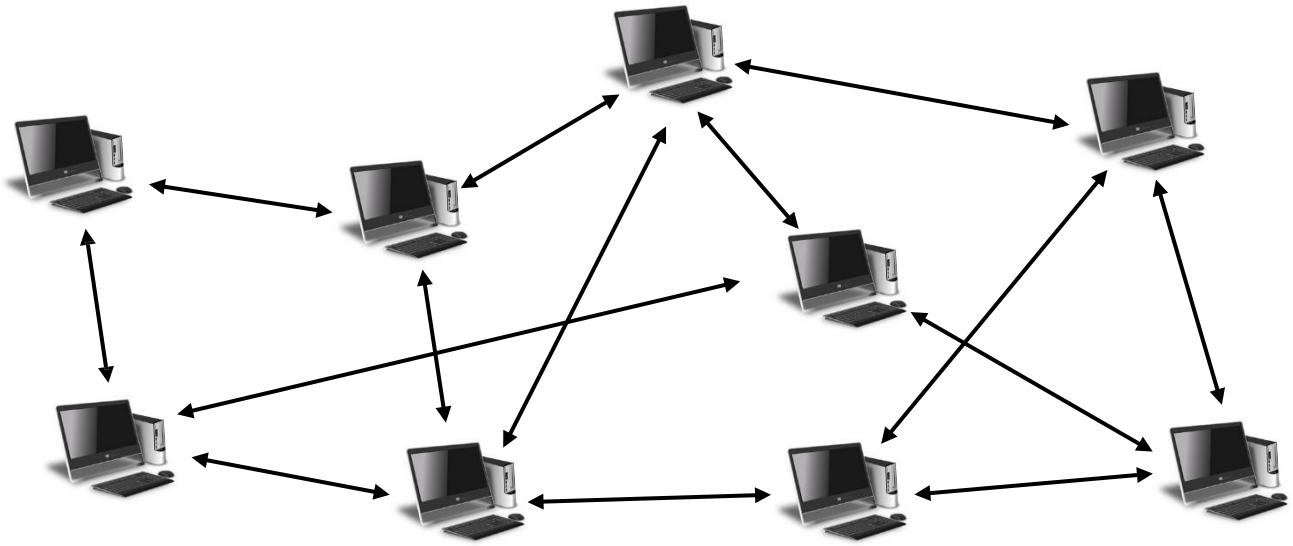
IPFSにおけるSybil攻撃のオンデマンド検知

立命館大学　情報理工学部
姫野貴一・上山憲昭

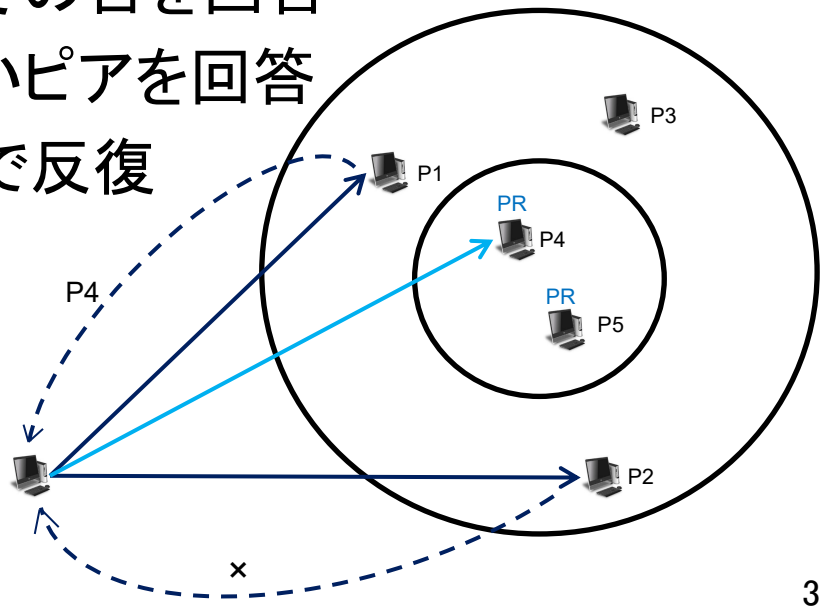
IPFS(InterPlanetary File System)

- P2Pネットワーク上で，完全自律分散でデータを分散して保存するシステム　→　Web3が目指す分散型ウェブデータ共有システム
- DHT（distributed hash table）を用いてコンテンツの取得を行う
- 本質は「権威的サーバのない自律分散型の名前解決メカニズム」
  - すべてのノードが対等な立場で振る舞い、データやコンテンツのやり取りを行う



IPFSのコンテンツ取得の流れ

- IPFSはDHTを用いてPUTとGETの対象ピアを選択
- 各ピアはルーティングテーブル(PIDとIPアドレスの組)を保持
- DHT探索処理(DHTウォーク)
  - ノードは自身のルーティングテーブルからCIDとのXOR距離が近い10個のピアを選出、並列に問い合わせ
  - 問い合わせを受けたピアの動作:
    - 自身がCIDのデータを保持 ⇒ その旨を回答
    - そうでない場合 ⇒ 自身より近いピアを回答
  - ProviderRecord(PR)を見つけるまで反復



IPFSの優位性・課題

優位性

- 分散性：中央管理者を必要とせず、耐検閲性・耐改ざん性に優れる
- 拡張性：既存のWebやアプリケーションに統合でき、Web3の基盤として活用可能
- 障害耐性

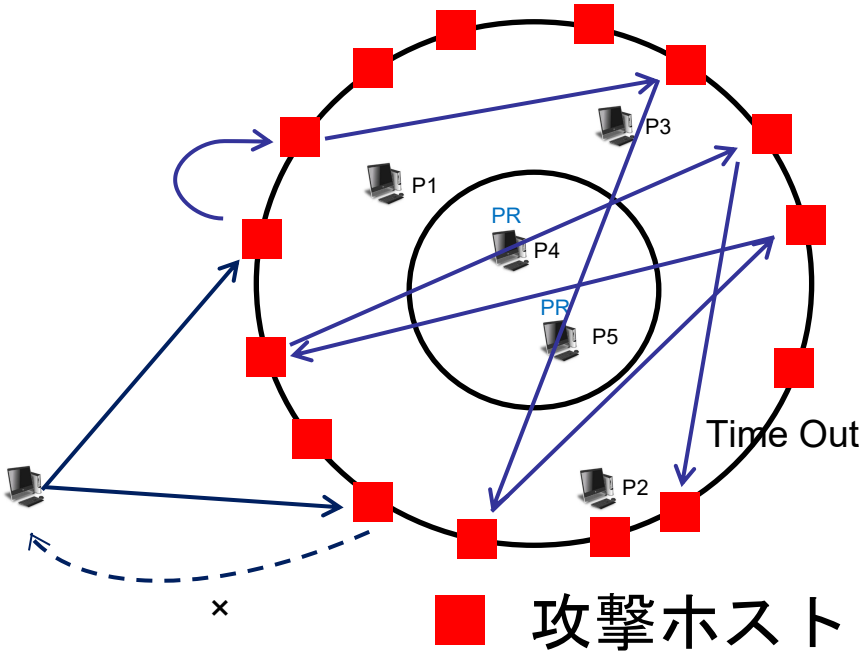
課題

- Sybil攻撃への耐性がない

研究の背景

- Sybil攻撃
  - 攻撃者は，特定のターゲットCIDにXOR距離が近いPIDを有する攻撃ホストを大量にIPFSに接続

- ターゲットCIDの取得時に要求が攻撃ホストへ集中し，攻撃ホストは正当なノードを返さず，他の攻撃ホストを応答することで要求を循環させる。結果として，要求者は目的のCIDに到達できない。



本研究の目的・既存研究の紹介

- 既存研究のアプローチ
  - Push時検知：コンテンツをネットワークに公開する際に検知
  - 定期検知：一定の時間間隔ごとに全体を走査して検知
  - 遅延ベース検知：ユーザのコンテンツ要求から取得完了までの時間遅延を指標に検知

- 本研究の目的:定期検査は無駄が多く、push時検知は後出しSybilを検出できず、遅延ベース検知は時間と誤検知の問題を抱える。そこで本研究では、要求発生時のみ計測を行うオンデマンド検知を導入し、検知コストを抑えその検知精度とコスト効果を評価する。

アプローチ（1/2）

- 本研究のアプローチ（オンデマンド検知）
  - ユーザ要求をトリガー：コンテンツ要求が発生した時のみ検知を実施
    - 人気コンテンツ：要求回数が多いため検査頻度が上がり、検知率を高められる
    - 不人気コンテンツ：不人気コンテンツはリクエストが少ないため、検査が最小限でコストを抑えられる。

アプローチ(2/2)

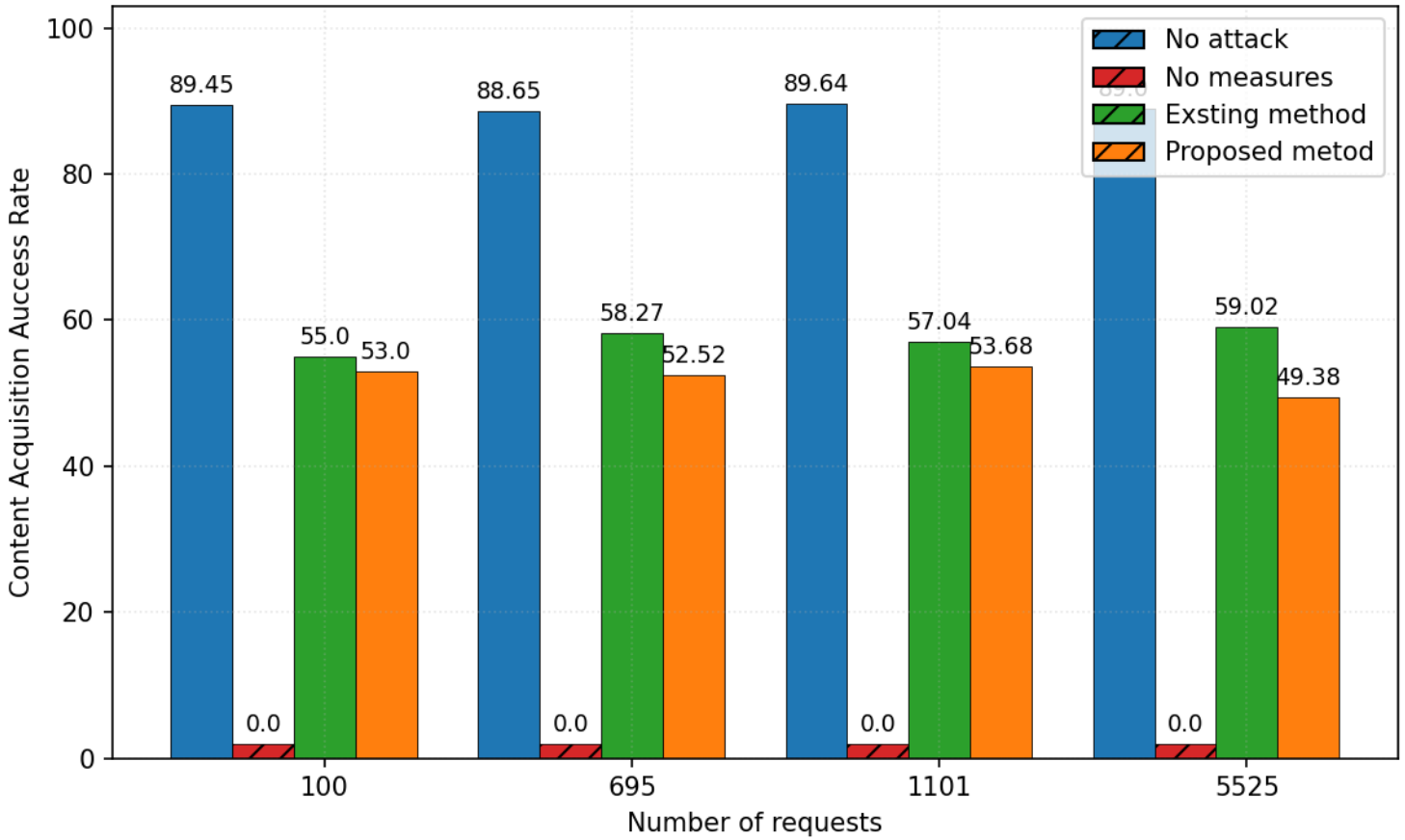
- 分布のエントロピーに基づく検知
  - KLダイバージェンスを利用：要求対象CID周辺のPeer ID（PID）分布を観測
    - 正常時の分布と比較
    - エントロピー差から攻撃の有無を判定
  - $\mathrm{D}_{KL}(P||Q) = \sum_{i=1}^{n} p_i log_2 \frac{p_i}{q_i}$
    - P=$\{P_i\}$：観測分布
    - Q=$\{q_i\}$：基準分布

評価概要

- 評価概要
  - コンテンツ取得率を指標とした性能評価
  - 要求数に対する取得率の変化を分析
  - ホップ数の違いによる影響も併せて評価

性能評価（1/2）

- 検知頻度を抑制しつつ、コンテンツ取得成功率を維持



性能評価（2/2）

- 全体結果の比較
- 攻撃なし環境：

  コンテンツ取得率：88.24%　平均ホップ数：2.17
- 既存研究手法：（調査回数　480,000）

  コンテンツ取得率：74.08%　平均ホップ数：2.53
- 提案手法：（調査回数　100,000）

  コンテンツ取得率：74.18%　平均ホップ数：2.52

まとめ

- 提案手法により、検知コストを抑制しつつ、コンテンツ取得成功率および平均ホップ数を高い水準で維持することを実現
  - 既存の検知アルゴリズムでは防御コストが高くスケーラビリティに課題

- 課題
  - KLダイバージェンスの閾値設定およびProvider Record再配布間隔の最適化が十分でなく、特に高人気コンテンツにおける取得効率向上が限定的であった点が挙げられる

参考文献

- Active Sybil Attack and Efficient Defense Strategy in IPFS DHT (Nettoら, 2025, arXiv)
- Web3 Sybil Avoidance Using Network Latency（Stokkinkら, 2023, *Computer Networks*）
- Mapping the Interplanetary Filesystem（Henningsenら, 2020, arXiv）
- IPFS – Content Addressed, Versioned, P2P File System（Benet, 2014, arXiv）
- Sybil Attack Strikes Again: Denying Content Access in IPFS (Cholez & Ignat, arXiv)