An Optimal Statistical Test for Robust Detection against Interest Flooding Attacks in CCN

Tan NGUYEN Remi COGRANNE Guillaume DOYEN

ANR DOCTOR project, number <ANR-14-CE28-000>
Troyes University of Technology, France
{ngoc_tan.nguyen, remi.cogranne, guillaume.doyen}@utt.fr

14th IFIP/IEEE Symposium on Integrated Network and Service Management 2015

Outline

Outline

Information Centric Network (ICN)

- Internet usage keeps growing tremendously
- Recent efforts aiming to a clean-slate network for the future

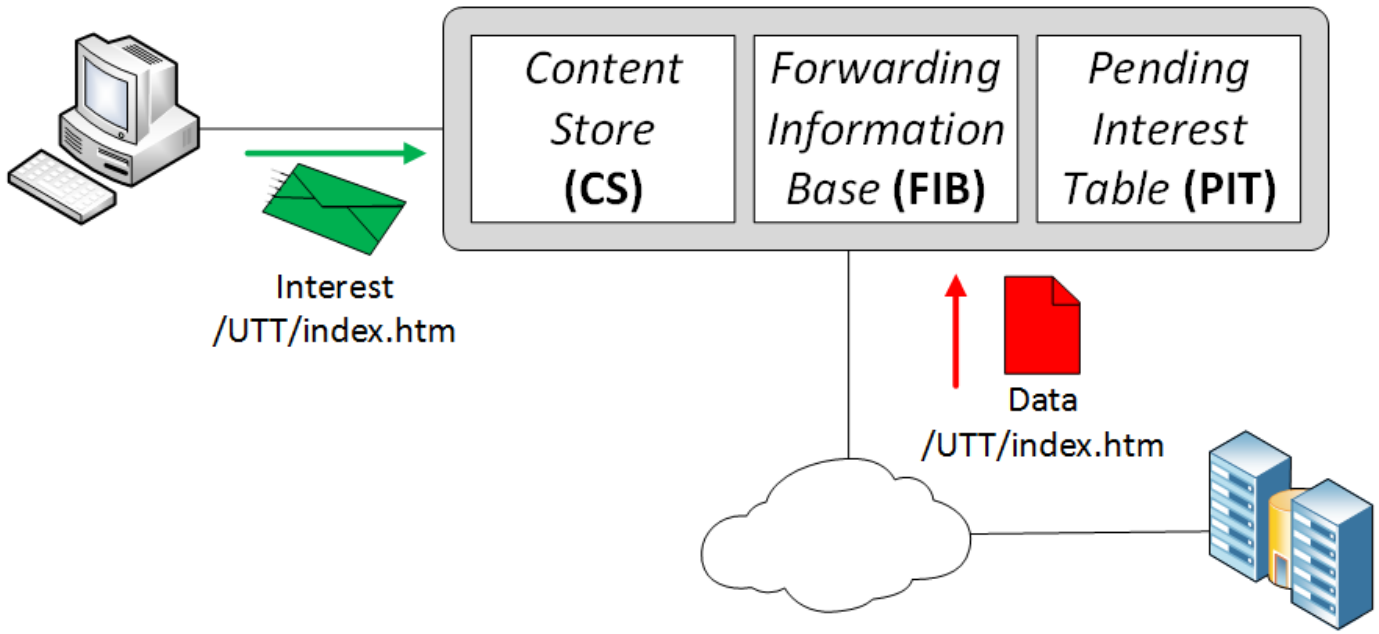
ICN key concepts

- Naming content object instead of using IP address
- In-network caches
- Ensure content integrity, authenticity

- Natively solve part of problems: multicast, mobility support, IP address shortage ...

Content Centric Network (CCN)

- Promising future network architecture
- Communications by *Interest* and *Data* packets



Outline

Interest flooding

- A Denial-of-Service variation in CCN environment

Attack principle

Overload **PIT** with a large amount of Interests for **non-existent content names**, prevent router from processing Interests from legitimate user

- Highly risk
  - Non-existent name can be easily created
  - Can effect on large scale

Previous work

- Proposed solutions against Interest flooding exist [1] [2] [3]
- A combination of both reliable detector and effective countermeasure still missing

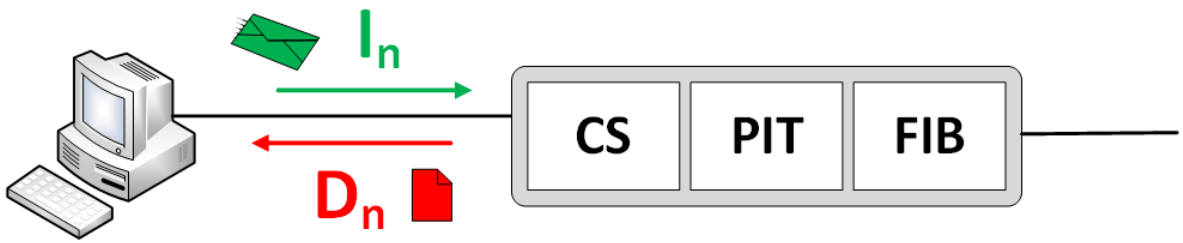
Previous detection method's drawbacks

- Unclear threshold selection, usually based on experiences
  - ⇒ **Rigid performance, only valid in evaluated cases**
  - ⇒ **Costly to address different conditions**
- No expected theoretical performance
  - ⇒ **Achieved results under-optimal**
- Evaluate with easily detected cases
  - ⇒ **Unreliable and weak performance against challenge cases**

Outline

Methodology

Statistical Hypotheses Testing with Neyman-Pearson approach



Assumptions

- $I_n \sim \Pi(\lambda)$; $D_n \sim B(I_n; p_0)$
- Parameters p_0, λ constant, already known
- Values of D_n *statistically independent*
- Additional malicious Interests issued by attacker $i_n \sim \Pi(a)$
- Links' and content providers' capacity is sufficient

Method's key concepts

- **False-alarm rate** α: false positives
- **Detection power** β: true positives
- **Miss-detection rate** $1 - \beta$: false negatives
- **Uniformly Most Powerful (UMP) test** is a test achieve the best β for a given α
- **Detection threshold** τ

Problems of previous work

τ, α *and* β come after empirical data of particular cases and the detector is not the uniformly most powerful

Proposed detection method

Proposed UMP detector

$$\mathcal{X} = \sum_{i=1}^{N} X_n = \sum_{i=1}^{N} \frac{D_n - I_n.p_0}{\sqrt{I_n\, p_0(1-p_0)}}$$

$$\text{Interface is } \begin{cases} \text{normal if } \mathcal{X} \geq \tau \\ \text{under attack if } \mathcal{X} < \tau \end{cases}$$

Threshold & expected detection power

$$\tau = \Phi^{-1}(\alpha)\sqrt{N}$$

$$\beta = \Phi\left(\frac{\Phi^{-1}(\alpha)\sqrt{N} - N\mu_1}{\sigma_1\sqrt{N}}\right)$$

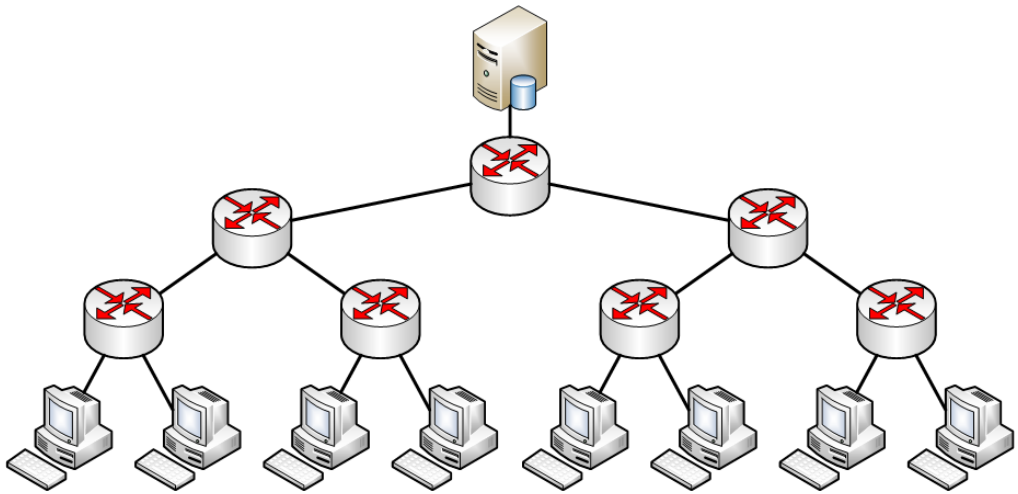
Outline

Evaluation setup

- Reuse ndnSIM source code of competitor and modify it to integrate all the configuration

Our competitor

Afanasyev, Alexander, et al. "Interest flooding attack and countermeasures in Named Data Networking." IFIP Networking Conference, 2013. IEEE, 2013.



Approach relevance

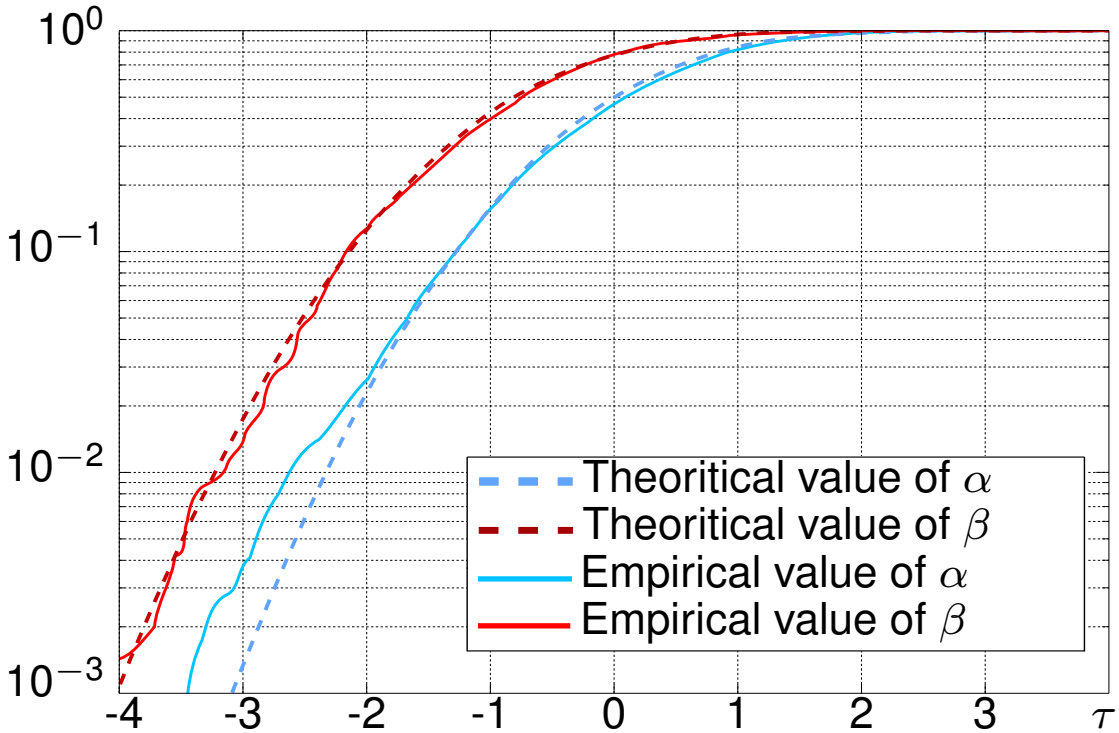


Figure: Theoretical and empirical α and β as a function of threshold τ.

Performance comparison

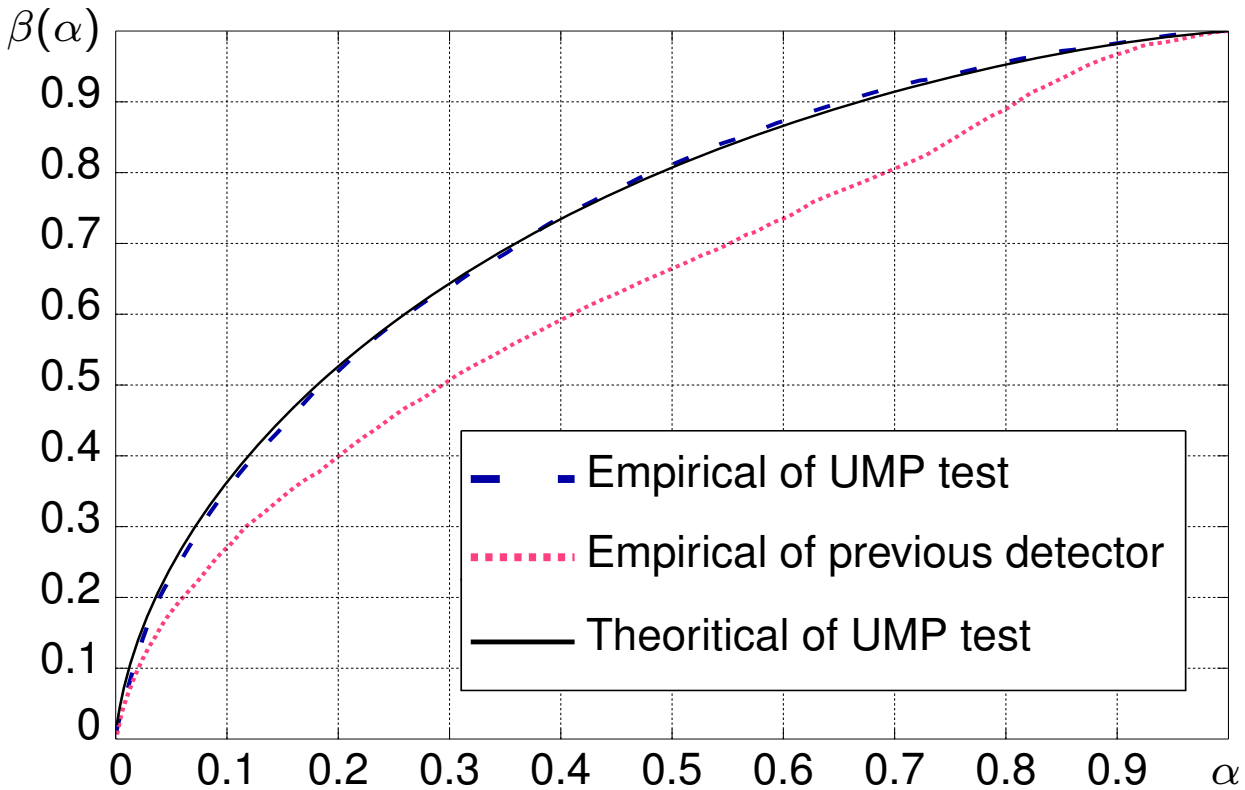


Figure: Overall performance of UMP test and the satisfaction ratio D_n/I_n test.

Identifying challenge cases

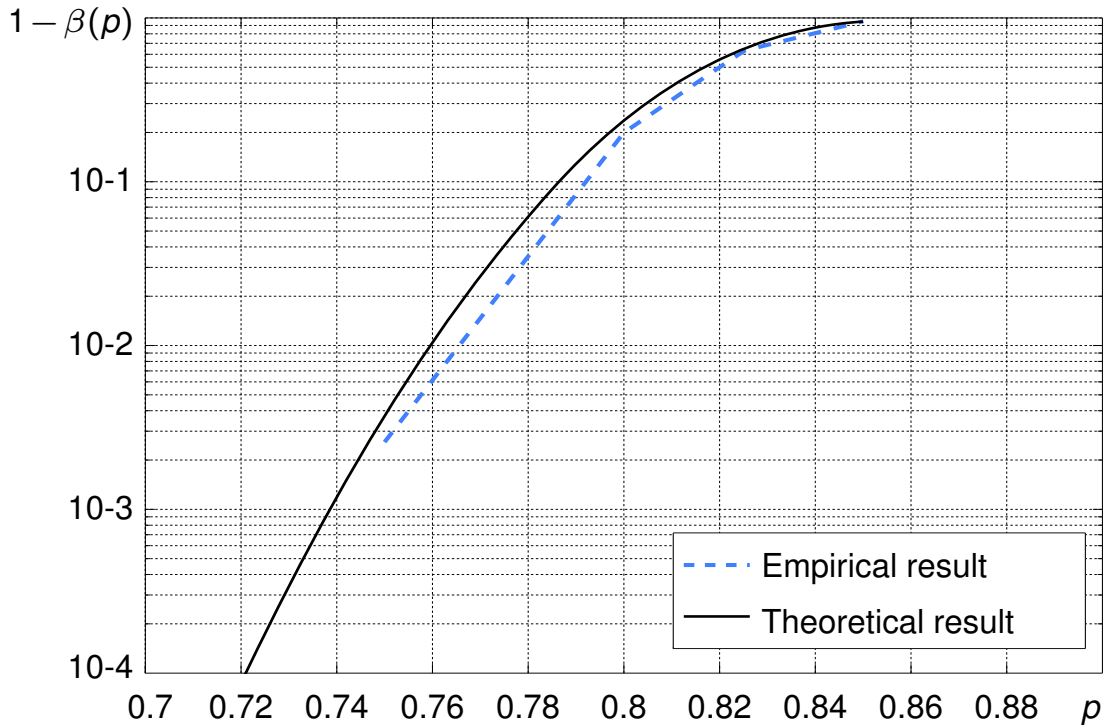


Figure: Empirical and theoretical $1-\beta$ of the UMP test, for a single host, as a function of p. Here $\alpha = 0.05$, $N = 1$ and $p_0 = 0.85$.

Potential improvement for challenge cases

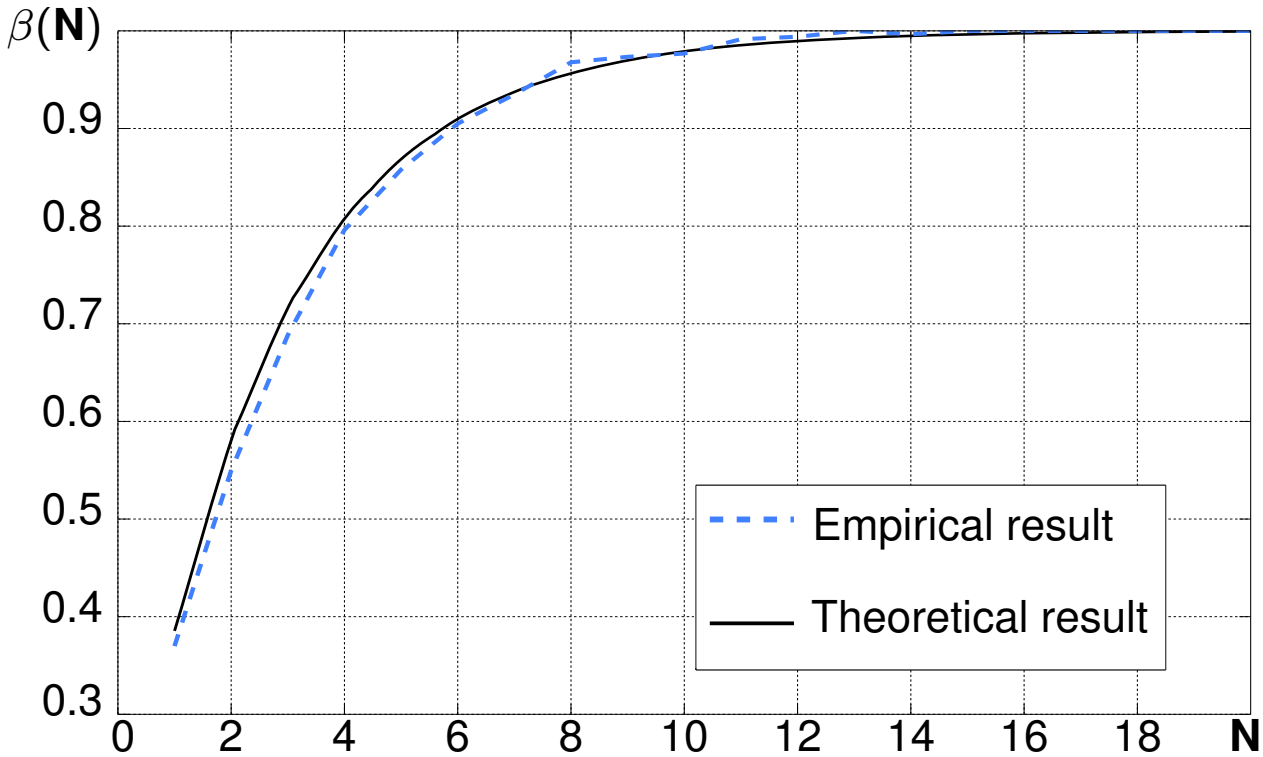


Figure: Empirical and theoretical β of the UMP test as a function of sample size N. Here $\alpha = 0.05$, $p_0 = 0.85$ and $p = 0.825$.

Outline

Conclusion & future work

The proposed detector

- Has a clearly-defined, scalable threshold
- Threshold independent of users' behavior, adaptable to α
- Has better performance, even in some challenge cases
- Provide a reliable theoretical performance
- Master the trade-off between accuracy and detection delay

Future work

- Address important-but-less-noticeable attack strategies
- Develop a mitigation strategy


Afanasyev, Alexander, Priya Mahadevan, Ilya Moiseenko, Ersin Uzun, and Lixia Zhang
Interest flooding attack and countermeasures in Named Data Networking
IFIP Networking Conference pp. 1-9. IEEE, 2013.


Compagno, Alberto, Mauro Conti, Paolo Gasti, and Gene Tsudik
Poseidon: Mitigating Interest flooding DDoS attacks in Named Data Networking
IEEE Conference on Local Computer Networks (LCN) pp. 630-638. IEEE, 2013.


Dai, Huichen, Yi Wang, Jindou Fan, and Bin Liu
Mitigate ddos attacks in ndn by interest traceback
Computer Communications Workshops (INFOCOM WKSHPS) pp. 381-386. IEEE, 2013.