utt
université de technologie
Troyes

Agence Nationale de la Recherche
ANR

DOCTOR

Interest Flooding Detection in NDN using Hypothesis Testing

T. NGUYEN, R. COGRANNE, G. DOYEN, F. RETRAINT
Troyes University of Technology, France

IEEE International Workshop on Information Forensics and Security
Roma Tre University, Rome, Italy

Thursday 19 November, 2015

Outline of Presentation

1. Interest flooding attack in Named Data Networking
2. Detection Problem Statement
3. Interest flooding detection
4. Evaluation results
5. Conclusion & future work

Named Data Networking

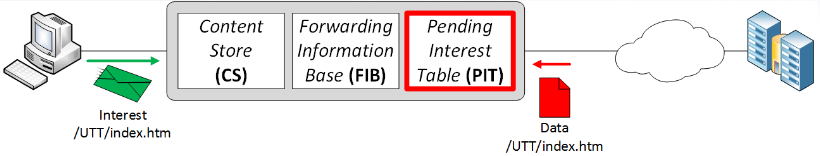
- Internet usage keeps growing tremendously
- Recent efforts aiming to a clean-slate network for the future
- NDN: promising future Internet

NDN 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 ...

- Communications by *Interest* and *Data* packets



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
  - Easily created
  - Potentially affect on large scale

- Proposed solutions usually include a detection phase followed by a mitigation step [1,2]

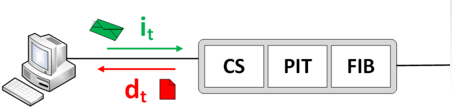
Previous detection method's drawbacks

- 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**

[1] A. Afanasyev et al. "Interest flooding attack and countermeasures in Named Data Networking." IFIP Networking Conference, 2013

[2] A. Compagno et al. "Poseidon: Mitigating interest flooding DDoS attacks in named data networking." IEEE Local Computer Networks (LCN), 2013.

Detection Problem Statement



Assumptions

- p_t: loss rate of a legitimate Interest
- $d_t \sim \mathcal{B}(i_t; 1 - p_t)$
- $\ell_t = 1 - d_t / i_t$: measured packet-loss rate

The two statistical hypotheses

- $\mathcal{H}_0$: no Interest flooding

$$\mathcal{H}_0 : d_t \sim \mathcal{B}\left(i_t, 1 - p_t\right)$$

- $\mathcal{H}_1$: an Interest flooding is occurring

$$\mathcal{H}_1 : d_t \sim \mathcal{B}\left(i_t - N_t, 1 - p_t\right) \, , \; N_t > 0$$

Outline of Presentation

- The case of **known loss rate** p_t already addressed
  $\Rightarrow$ upper bound for the detection performance

For the case of unknow loss rate

- Values of p_t changes slightly and smoothly
  $\Rightarrow$ Possible to model with a polynomial
- Consider N measurements $\boldsymbol{\ell} = (\ell_{T-N+1}, \dots, \ell_T)$
- Least-square estimator of packet-loss rate

$$\widetilde{\mathbf{p}} = \mathbf{H}\widetilde{\mathbf{x}} = \mathbf{H}(\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T\boldsymbol{\ell}$$

Reformulate the hypotheses

- $\ell_t = 1 - d_t/i_t$ and i_t usually large enough

Using Central Limit Theorem

$$\begin{cases} \mathcal{H}_0 : \boldsymbol{\ell} \rightsquigarrow \mathcal{N}\left(\mathbf{H}\widetilde{\mathbf{x}}\,,\ \boldsymbol{\Sigma}_0\right), \\ \mathcal{H}_1 : \boldsymbol{\ell} \rightsquigarrow \mathcal{N}\left(\mathbf{H}\widetilde{\mathbf{x}} - \mathbf{a}\mathbf{v}_a\,,\ \boldsymbol{\Sigma}_0 - \boldsymbol{\Sigma}_a\right) \end{cases}$$

where $\mathbf{a}$ represents the attack payload and $\mathbf{v}_a$ characterizes for the number of samples corrupted by the attack, e.g. $\mathbf{v}_a = (0, 0, \ldots, 0, 1)^T$

Estimated residual

$$\mathbf{H}^{\perp} = \mathbf{I} - \mathbf{H}(\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T$$

$$\widetilde{\mathbf{r}} = \boldsymbol{\ell} - \widetilde{\mathbf{p}} = \mathbf{H}^{\perp}\boldsymbol{\ell} \sim \begin{cases} \mathcal{H}_0 : \mathcal{N}\left(\mathbf{0}\,,\ \mathbf{H}^{\perp}\boldsymbol{\Sigma}_0\mathbf{H}^{\perp T}\right), \\ \mathcal{H}_1 : \mathcal{N}\left(\mathbf{a}\widetilde{\mathbf{v}}_a\,,\ \mathbf{H}^{\perp}\boldsymbol{\Sigma}_0\mathbf{H}^{\perp T} - \mathbf{H}^{\perp}\boldsymbol{\Sigma}_a\mathbf{H}^{\perp T}\right) \end{cases}$$

Generalized Likelihood Ratio Test (proposed GLRT)

$$\widetilde{\delta}(\widetilde{\mathbf{r}}) = \begin{cases} \mathcal{H}_0 & \text{if} \quad \widetilde{\mathbf{v}}_a^T \widetilde{\mathbf{r}} \leq \widetilde{\tau}, \\ \mathcal{H}_1 & \text{if} \quad \widetilde{\mathbf{v}}_a^T \widetilde{\mathbf{r}} > \widetilde{\tau}. \end{cases}$$

with: $$\widetilde{\mathbf{v}}_a^T \widetilde{\mathbf{r}} \rightsquigarrow \begin{cases} \mathcal{N}\left(\mathbf{0}\,,\, s_0^2\right) & \text{under} \quad \mathcal{H}_0, \\ \mathcal{N}\left(\mathbf{a}\|\widetilde{\mathbf{v}}_a\|_2^2\,,\, s_0^2 - s_a^2\right) & \text{under} \quad \mathcal{H}_1. \end{cases}$$

and: $$s_0^2 = \widetilde{\mathbf{v}}_a^T \mathbf{H}^{\perp} \boldsymbol{\Sigma}_0 \mathbf{H}^{\perp T} \widetilde{\mathbf{v}_a}\,, \quad s_a^2 = \widetilde{\mathbf{v}}_a^T \mathbf{H}^{\perp} \boldsymbol{\Sigma}_a \mathbf{H}^{\perp T} \widetilde{\mathbf{v}_a}.$$

Threshold & expected detection power

Threshold: $$\widetilde{\tau} = \Phi^{-1}\left(1 - \alpha_0\right) s_0$$

Detection power: $$\beta(a) = 1 - \Phi\left(\frac{s_0 \Phi^{-1}(1-\alpha_0) - a\|\widetilde{\mathbf{v}}_a\|_2^2}{\sqrt{s_0^2 - s_a^2}}\right)$$

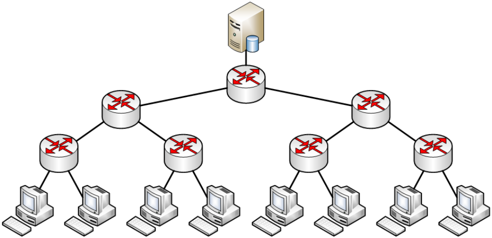
Evaluation setup

Test configuration

- $N = 50$ and $q - 1 = 4$
- $\mathbf{v}_a = (0, 0, \dots, 0, 1)^T$

Experiment setup

- Using data generated in ndnSIM
- $i_t \sim \Pi\{\lambda\}$ and $N_t \sim \Pi(a)$, with $\lambda , a \sim unif$
- Links' and content providers' capacity is sufficient
- Actual packet-loss rate follows an auto-regressive model: $p_t = p_{t-1} + u$ with $u \sim unif$



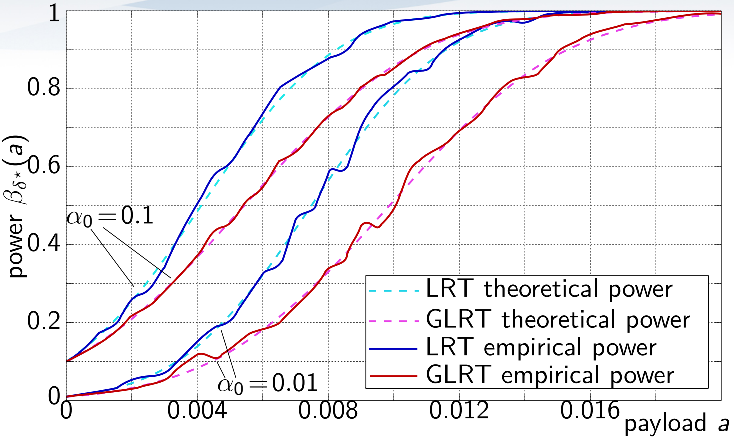


Figure: Comparison of theoretical and empirical performance of LRT and proposed GLRT, as a function of anomaly strength $a \in [0, 0.02]$.

Guaranteeing False Alarm Probability

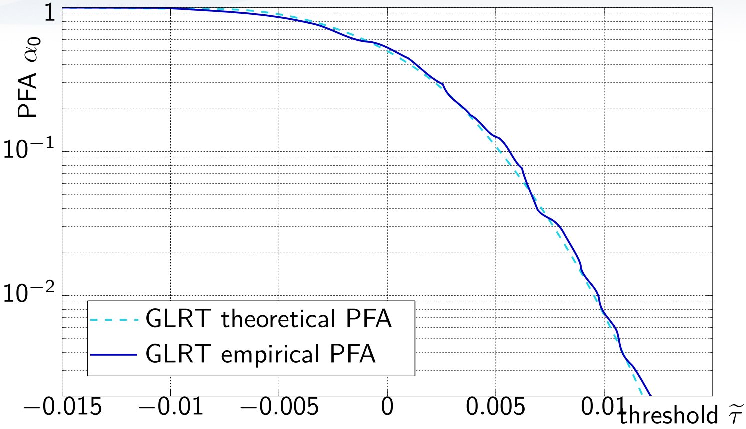


Figure: Comparison between empirical and theoretical PFA for the proposed GLRT, as the function of decision threshold $\widetilde{\tau}$.

Trade-off between detection latency and power

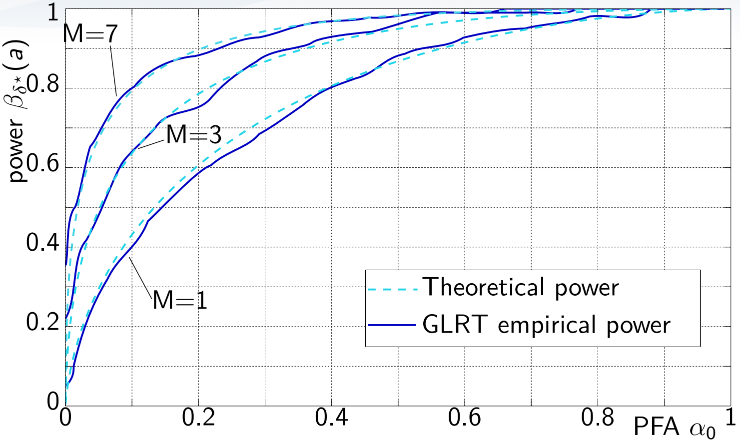


Figure: Receiver Operational Characteristic (ROC) curves for the proposed GLRT with different number of samples corrupted.

Outline of Presentation

1. Interest flooding attack in Named Data Networking
2. Detection Problem Statement
3. Interest flooding detection
4. Evaluation results
5. Conclusion & future work

Conclusion & future work

The proposed detector

- Has a clearly-defined threshold which can guarantee a prescribed α_0
- Threshold independent of users' behavior or attack payload
- Provide a reliable theoretical performance, hence allow evaluating the loss in detection power due to estimation
- Master the trade-off between accuracy and detection delay

Future work

- Address other important attack strategies
- Develop a following mitigation strategy