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

Tan NGUYEN
ICD - ROSAS - STMR
Troyes University of Technology,
UMR 6281, CNRS
10004 Troyes cedex - France
Email: ngoc_tan.nguyen@utt.fr

Remi COGRANNE
ICD - ROSAS - LM2S
Troyes University of Technology,
UMR 6281, CNRS
10004 Troyes cedex - France
Email: remi.cogranne@utt.fr

Guillaume DOYEN
ICD - HETIC - ERA
Troyes University of Technology,
UMR 6281, CNRS
10004 Troyes cedex - France
Email: guillaume.doyen@utt.fr

***Abstract*—Confronting the changing demand of users, the current Internet is revealing its limitations. Information Centric Network (ICN) are Future Internet proposals which are based on named data objects. In order to actually replace its predecessor, ICN must be able to resist existent threats in the current Internet, especially the Denial of Service (DoS) attack. In this paper, we focus on Interest flooding - a new type of DoS attack in Content Centric Network (CCN). Several solutions for this threat have been introduced, but they do not solve the problem in a satisfying way because of some drawbacks in either their detection performance, scalability support or restricted scenario of usage. Our goal is to design a reliable, low resources-consuming detection method against Interest flooding attack in CCN. A detection scheme must be attended since a lot of resources consumed by unnecessarily continuous countermeasure can be saved by a dependable detector. Like no other detectors in proposed solutions, our detector is based on statistical hypotheses testing theory. The achieved result is a low resources-consuming detector that can be deployed globally on each CCN router. The false alarm probability of our detector can be controlled at will. Its statistical power can be theoretically established and evaluated precisely. To validate our contribution, numerical results show the relevance of the proposed approach and the sharpness of theoretical results.**

I. Introduction

The Internet users' demand to access content and the growth of mobile traffic is increasing unexpectedly. According to Cisco's forecast[1], in 2013, the consumer Internet video traffic was 18 Exabytes (EB)[2] per month, equivalent to 62% of all consumer Internet traffic (including fixed and mobile network). The forecast predicts that in 2018, this amount will reach 64.7 EB, contributing 78% to all consumer Internet monthly traffic. The mobile traffic generated 1.48 EB in 2013, contributing 3% to global fixed and mobile data traffic. In 2018, the mobile traffic is expected to grow to 15.838 EB, accounting for 12% global data traffic. However, our current Internet was originally designed for accessing a specific computer system at distance, not for those emerging requirements. That is the reason why Information Centric Network (ICN) [1] [2] are crucial at this moment. By multi-casting and deploying in-network caches, ICN reduces the significant load on servers and routers in the face of increasing demand for data access. To solve the problem of mobility, ICN establishes communications based on named data objects, not on location-related IP addresses. Such communications are more flexible since they are not necessarily maintained end-to-end overtime.

In spite of being considered as the promising future of Internet, ICN proposals are still under development and cannot avoid flaws in operations, especially in security. Each ICN proposition has different security problems. We focus on the *Interest flooding* [3] in *Content Centric Network* (CCN) [4]. Interest flooding mainly impacts on routers, data providers and can be launched easily without much knowledge of the target network. Although several solutions have been proposed for this problem, they are not suitable for a deployment in reality because of their unreliable and rigid detection method as well as resources-consumption.

The contribution of this paper is to address the Interest flooding attack with a detection scheme based on *Statistical Hypothesis Testing Theory* which was never used before by other proposed solutions. The strengths of the proposed detector are: (1) scalability; (2) controllability of false alarm probability and (3) analytically established evaluation. First, the proposed detection method is simple enough so that is can be deployed in reality without using up too much resources on routers. Secondly, the statistical properties of the proposed detection method is analytically established, allowing the control of false alarm probability. In other words, our detector can be modified without causing more false alarms unintentionally. Thirdly, statistical hypothesis testing theory makes our evaluation well-grounded and more reliable since the empirical result can be compared with the theoretical one. ndnSIM [5] - an open source NS-3 based simulator for CCN network - was selected to generate data for our evaluation. The numerical results from simulations show that our detector provides a great overall performance which is similar to the theoretically established performance. Also, the proposed detector nearly reaches the theoretically established power in most of the cases.

The rest of this paper is organized as follows. Section II presents related work, including an overview of ICN propos-

[1]http://www.cisco.com
[2]1EB = 10^6 TB

als, CCN's operations and an overview of security issues in ICN. Section III introduces our proposed detection method for Interest flooding in CCN and establishes analytically its statistical performance. Section IV evaluates the performance and the power of the proposed detector in our set up with simulated data from ndnSIM. Finally, Section V concludes the paper and presents our work in future.

II. Related works

In this section, we briefly introduce ICN's key concepts, CCN's operation and its security issues, with a focus on the Interest flooding attack and its recently proposed solutions.

A. *Information Centric Network*

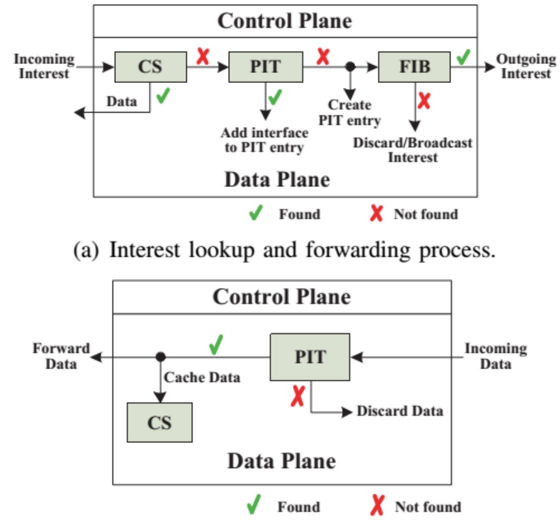
ICN is a networking paradigm which is based on data objects. The key concept in ICN is that it names each data object in the network, instead of using IP addresses for naming hosts and nodes. Secondly, a node in ICN does not have to connect to one specific server to get data. Alternately, this node will send a request with the name of the required data object. Then, the network will return the corresponding object to this node. The third key concept is that ICN deploys in-network caching. Every time a packet passes a network elements, it will be cached. Based on these concepts, many ICN architectures have been introduced, including: DONA [6], CCN, PSIRP [7], NetInf [8].

Among ICN proposals, CCN is the most popular one in research community[3]. Besides, it allows researchers to evaluate their results with both implementations (e.g. CCNx[4]) and simulators (e.g ndnSIM [5]). In CCN, communications are based on requests for hierarchical content names and are performed by two type of packets: *Interest* and *Data*. A user sends an Interest packet when he wants to retrieve content and will receive a Data packet in return.

A *Content Router* (CR) in CCN includes three main data structures: (1) *Forwarding Information Base* (FIB); (2) *Content Store* (CS) and (3) *Pending Interest Table* (PIT). The FIB works like a routing table in a CR, while the CS acts like a local cache inside, storing every Data packet passing through. The PIT maintains a routing state for each forwarded Interest packet and uses these states to forward the corresponding Data back to the requester. A PIT entry contains a CCN name and multiple incoming interfaces. Figure 1(a) presents the Interest lookup and forwarding process in CCN. Whenever a CR receives an Interest for a content name, the CR will check the CS first. If a cached copy exists, the CR will send this copy back to the incoming interface. If a cached copy doesn't exist but a PIT entry for this content name is already created, the incoming interface of the Interest will be added to this entry and Interest will be dropped. If a matching PIT entry doesn't exist, a new entry will be created and then the

[3]Named Data Networking (NDN)[4] is an ICN architecture which is built on CCN ground and also gained a lot of popularity. However, since we only make use of the common fundamentals of these two projects in our work, we consider them equivalent.

[4]www.ccnx.org



(a) Interest lookup and forwarding process.

(b) Data lookup and forwarding process.

Fig. 1. Packet lookup and forwarding process in CCN [9]

Interest will be forwarded using routing information in FIB. If no matching route is found, the Interest can be discarded or broadcast, depending on the routing policy of the CR.

Figure 1(b) presents the Data lookup and forwarding process in CCN. When a CR receives a Data packet, it checks the PIT. If a matching PIT entry is found, it will cache the Data packet before forwarding it to all the corresponding interfaces in the PIT entry and then this entry will be removed. If the CR did not request for this Data, there is no matching PIT entry and the Data packet is dropped. The whole process ensures that one Interest only results in one Data packet.

B. *Security issues in ICN*

Regarding new components in CCN, the research community has revealed many security issues in CCN. In [10], Lauinger has pointed out how Content Store can be exploited to retrieve private information Data as well as some other cache-related issues. In [16], Goergen et al. design the first CCN-compliant firewall which can filter packets according to both their authentication and the semantics of the content name. In [17], Khan et al. address the necessity of a proper key management scheme in CCN and propose an online public key generation technique for the CCN architecture. In [3], Afanasyev et al. has indicated that the PIT can also be depleted, leading to a Denial of Service (DoS) in CCN. The principle of DoS attack in CCN is simple: sending a lot of Interests with nonexistent content names to make PIT overloaded. Hence, the DoS attack in CCN has a different name: Interest flooding attack. Also in this work, the authors explained why the two types of packets - (1) Data packets and (2) Interests with existent content names - are not appropriate for launching DoS attack in CCN. First, Data packets fail to launch a DoS attack in CCN because a CR refuses to forward Data that it did not request for. Secondly, Interests with existent content name also fail to launch this attack since the next requests for the same existent content name will be satisfied by caches instead of being forwarded toward content providers. By forging nonexistent content names, attacker can target a specific content provider or can aim to sabotage the network infrastructure. In addition, Interest flooding attack has a high risk because nonexistent names can be easily created without much knowledge about the network and data.

Several solutions for detecting and mitigating against Interest flooding attack have been proposed. In [9], Dai et al. present their Interest trace back mitigation strategy. Whenever the PIT's size exceeds a threshold, a spoofed Data packet is created by the CR to respond a long-unsatisfied Interest. These Data are eventually forwarded back to the source of attack by tracing PIT entries. At the same time, CRs also limit the incoming packet rate of interfaces to which they sends fake Data.

In [11], Tang et al. aim to identify the compromised name prefixes which are used to launch *Interest* flooding, and then announce these malicious prefixes to neighbors. There are two phases: (1) rough detection and (2) accurate detection. In the rough detection, malicious interfaces are detected by computing a *satisfaction ratio* - a ratio between number of outgoing Data and incoming Interests on an interface. When this ratio exceeds a threshold, the interface is considered under attack. The threshold of this phase is pre-configured for all cases. In the accurate detection, expired Interests on the reported interface are recorded. The prefix that has the largest expired ratio is considered hostile.

Having the same idea of using statistics to identify harmful interfaces, the Poseidon approach, proposed by Compagno et al. in [12], maintains two measures: (1) the satisfaction ratio and (2) the PIT space used up by *Interests* from the concerned interface. Once an alarm occurs, a CR issues an alert message to its neighbor on the malicious interface. When a CR receives an alert, it also triggers the same countermeasure, but with a lower threshold, in order to better identify the compromised interface.

Among all these proposed detection and mitigations strategies, the satisfaction-based push back [13] is the most notable one. The idea of this proposal is the same as Poseidon proposal: routers exchange announcements to neighbors and adjust their reactions based on these messages. Although this solution monitors the satisfaction ratio, it does not have a separate detection phase. The ratio is actually used to periodically calculate the Interest limit exchanged in announcements between routers.

In spite of using different methods, all the presented solutions have some common drawbacks. Firstly, most of them use threshold for detection, but none of them can indicate reliably how the threshold value is set. A poorly-defined threshold can result in a rigid and untrustworthy detector that wastes router's resources for reactions to false alarms. Secondly, the majority of proposed solutions require routers' co-operation, making them depend on each other. Hence, when a router is compromised, it can sabotage communications in the network by sending false announcements to its neighbors. Then these neighbors may also spread these false messages to other routers in the network.

TABLE I
NOTATIONS AND SYMBOLS

Notation	**Meaning**
N	Sample size
I_n	Number of incoming Interests at time n^{th}
D_n	Number of outgoing Data at time n^{th}
p_0	Hit rate of each Interest under normal case
p	Hit rate of each Interest under attack
λ	Mean rate of traffic from a legitimate user
a	Mean rate of malicious Interests
$\mathcal{H}_0$	Null hypothesis
$\mathcal{H}_1$	Alternative hypothesis
PFA, α_0	Probability of False Alarm
α	Prescribed PFA
β	Detection power
τ	Threshold of the detector
δ	Statistical test
$\tilde{\delta}$	Uniformly Most Powerful test
$X \rightsquigarrow Y$	X converge in distribution to Y
$\lfloor x \rfloor$	The greatest integer less than or equal to x

By using statistical hypothesis testing theory, we have overcome these drawbacks and provide a detector with a well-defined threshold that works independently on each router. Moreover, we can control the false alarm probability of our detection scheme and estimate its statistical power precisely.

III. SIMPLE STATISTICAL METHODOLOGY FOR ANOMALOUS TRAFFIC DETECTION IN CCN

In this section, we present our proposed detection method for Interest flooding attack in CCN. The goal of our work is to design a reliable low resources-consuming detector so that it can be globally deployed for each interface of each router. A detection scheme is attended in our work since a lot of resources consumed by unnecessarily seamless reactions could be saved by a trustworthy detector.

A. Statistical hypothesis testing theory

The method we used to design our detection is based on statistical hypothesis testing theory with *Neyman-Pearson two-criteria* approach since it can provide a consistent most powerful test that does not depend on router's characteristics or measured values. Besides, this statistical approach allows establishing false-alarm, missed detection probabilities and, hence, setting up a threshold such that the prescribed performance can be ensured. Moreover, this method allows us to compare the empirical performance of our test with the theoretically established one, rendering the proposed test well-grounded and more reliable.

The input of hypothesis testing is a sample $\mathbf{Z}_N$, $\mathbf{Z}_N \in \mathcal{Z}$. This sample is a set of N empirical realizations of a random variable z. A *statistical hypothesis* $\mathcal{H}_j$ refers to a set of parameters vectors Θ_j. Each vector θ in this set defines a possible probability distribution $\mathbb{P}_\theta$ of $\mathbf{Z}_N$ [14]:

$$\mathcal{H}_j \;=\; \{\; Z_N \;\sim\; \mathbb{P}_\theta,\; \theta \;\in\; \Theta_j\}.$$

A hypothesis $\mathcal{H}_j$ is called *simple* when there is only one unique θ in Θ_j. On the contrary, it is called *composite*. In the usual case of binary statistical tests, there are two hypotheses: (1) *null hypothesis* $\mathcal{H}_0$ and (2) *alternative hypothesis* $\mathcal{H}_1$. $\mathcal{H}_0$ is usually the normal case and $\mathcal{H}_1$ is usually the abnormal case that we want to detect. A *statistical test* δ between two hypotheses $\mathcal{H}_0, \mathcal{H}_1$ is a subjective and measurable mapping from the sample space $\mathcal{Z}$ to the set of hypotheses [14]:

$$\delta :\; \mathcal{Z} \;\rightarrow\; \{\mathcal{H}_0, \mathcal{H}_1\}.$$

In order to design a good statistical test with the Neyman-Pearson approach, there are some key concepts which should be aware of: (1) probability of false alarm, (2) detection power, (3) Likelihood Ratio and (4) the uniformly most powerful test. The set Θ_0 defining $\mathcal{H}_0$ contains many parameters θ_0. For each of these parameters, there is a probability that the test δ rejects the null hypothesis $\mathcal{H}_0$ while it is actually true. The greatest value of these probabilities is called the *Probability of False Alarm* (PFA) of the test δ, denoted by $\alpha_0(\delta)$ [14]. Meanwhile, the *Detection Power* of a test δ, for a parameter $\theta_1 \in \Theta_1$, is the probability that $\mathcal{H}_1$ is detected correctly, denoted by $\beta(\theta_1, \delta)$ [14]:

$$\begin{aligned} \alpha_0(\delta) \;&=\; \sup_{\boldsymbol{\theta_0}\in\boldsymbol{\Theta}_0} \mathbb{P}_{\theta_0}\Big[\delta(\mathbf{Z}_N) = \mathcal{H}_1\Big], \\ \beta(\theta_1, \delta) \;&=\; \mathbb{P}_{\theta_1}\Big[\delta(\mathbf{Z}_N) =\; \mathcal{H}_1\Big]. \end{aligned}$$

For a prescribed false alarm probability α, we define the class of test $\mathcal{K}_\alpha$ containing all the tests whose false alarm probability is lower than α:

$$\mathcal{K}_\alpha = \Big\{\delta : \alpha_0(\delta) \le \alpha\Big\}.$$

A *Uniformly Most Powerful* (UMP) test $\tilde{\delta}$ in the class $\mathcal{K}_\alpha$ is a test providing the highest power under all the parameters $\theta_1 \in \Theta_1$ [14]:

$$\forall\delta \in \mathcal{K}_\alpha, \quad \forall\boldsymbol{\theta}_1 \in \boldsymbol{\Theta}_1, \quad \beta(\boldsymbol{\theta}_1; \delta) \le \beta(\boldsymbol{\theta}_1; \tilde{\delta}).$$

For simple hypotheses, since θ is unique for each hypothesis, the test $\tilde{\delta}$ is called the *Most Powerful* (MP) test.

The idea of Neyman-Pearson two-criteria approach is to design a test in the class $\mathcal{K}_\alpha$ that can warrant a pre-defined false alarm probability α and maximizes the test power $\beta(\theta_1, \delta)$. In the case of simple hypotheses, according to the Neyman-Pearson lemma [14], the most powerful test $\tilde{\delta}$ is the *Likelihood Ratio* (LR) test:

$$\tilde{\delta}(Z_N) = \begin{cases} \mathcal{H}_0 & \text{if } \Lambda(Z_N) \;=\; \frac{f_1(\mathbf{Z}_N)}{f_0(\mathbf{Z}_N)} \;< \tau, \\ \mathcal{H}_1 & \text{if } \Lambda(Z_N) \;\ge \tau \end{cases} \tag{1}$$

in which $\Lambda(\mathbf{Z}_N)$ is the LR and f_j is the probability density of $\mathbb{P}_j$, j = 0,1. LR test can be transformed by applying a monotone function to both side of the inequality in (1). The threshold τ is the solution of the equation:

$$\mathbb{P}_0\left[\Lambda(Z_N) \ge \tau\right] \;=\; \alpha.$$

Meanwhile, in the case of composite hypotheses, the UMP test barely exists in reality. The testing theory for this type of hypotheses is only well-developed for some particular cases. Due to the space constraint, only cases that are used to achieve the results will be presented.

B. Assumptions

At an interface of router, we measure two samples : (1) I_n - the number of incoming Interest at time n^{th} and (2) D_n - the number of outgoing Data packets at time n^{th}. We accept these assumptions for our models:

- I_n follows a Poisson distribution, denoted $\Pi(\lambda)$, since traffic streams on main communications arteries are accurately modeled by a Poisson process [15];
- The number of Data packets D_n follows a Binomial distribution, denoted $D_n \sim\; B(I_n; p_0)$ with $0 < p_0 < 1$. Not all the Interests can bring back a Data packet, for many reasons (e.g link's failure, request for wrong content names). Therefore, each Interest is considered as a Bernoulli trial with a probability p_0 of success. Since D_n is the sum of I_n Bernoulli trials with a probability of success p_0, it follows a Binomial distribution;
- Values of D_n are statistically independent. Two random variables are said to be *statistically independent* when knowing one does not convey any information about the other. This should not be confused with the term "unrelated". Although, Data packets can be related to each other in term of their content, knowing D_n will not provide any information about D_{n+1}. Hence, values of D_n are still statistically independent;
- The capacity of both links and content providers is assumed to be sufficient;
- If a host is compromised, it will send i_n additional Interests. These Interests request nonexistent names and do not return any Data. In order to become more subtle, the compromised host will facsimile the legitimate user's behavior. Hence, i_n also follows a Poisson distribution, denoted $\Pi(a)$;
- All the parameters p_0, a do not change over time for an interface and are known in prior.

C. Our proposed test

In our problem, $\mathcal{H}_0$ implies that "This interface is not attacked" while $\mathcal{H}_1$ implies that "This interface is under an Interest flooding attack". At first, the problem is solved as an original composite-hypothesis scenario. However, the resulting detector is not satisfactory because (1) it depends on I_n which varies in each measurement and (2) it is hardly scalable in reality. Specifically, this detector must be redesigned for each separate interface on which it is deployed. Besides, re-designing requires time and carefulness in order to provide a good performance. To resolve these drawback, the composite hypotheses are reformulated and resolved. The achieved result is a reliable low resources-consuming detector.

1) Composite-hypothesis approach: Under the normal circumstance - null hypothesis $\mathcal{H}_0$ - I_n and D_n should follow the distributions that we assumed above. Meanwhile, under $\mathcal{H}_1$, the mean of I_n increases since a compromised host will send addition Interests which do not bring back any Data packets. Meanwhile the hit ratio p_0 of each Interest remains unchanged, so the hit ratio under $\mathcal{H}_1$ becomes $p < p_0$:

$$\begin{aligned} \mathcal{H}_0\ \{p = p_0\}: \quad & I_n \sim\ \Pi(\lambda); \\ & D_n \sim\ B(I_n;\ p_0). \\ \mathcal{H}_1\ \{p < p_0\}: \quad & I_n \sim\ \Pi(\lambda\ +\ a); \\ & D_n \sim\ B(I_n;\ p). \end{aligned}$$

Notice that under both hypotheses, D_n follows a binomial distribution which belongs to a *one-parameter exponential distribution family* [14, Section 2.7]. This distribution family possesses a property [14, Corollary 3.4.1] that allows us to find out the following UMP test:

$$\tilde{\delta}(D_1, \ldots, D_n) = \begin{cases} \mathcal{H}_0 & \text{if } \sum_{n=1}^{N} D_n \geq \tau, \\ \mathcal{H}_1 & \text{if } \sum_{n=1}^{N} D_n < \tau. \end{cases} \tag{2}$$

The threshold τ is determined by the equation:

$$\mathbb{P}_{p_0}(\sum_{n=1}^{N} D_n \geq \tau)\ =\ \alpha. \tag{3}$$

Since $D_n\ \sim\ B(I_n, p)$, $\sum_{n=1}^{N} D_n$ is a sum of binomial distributions. Hence:

$$\sum_{n=1}^{N} D_n\ \sim\ B(\sum_{n=1}^{N} I_n, p). \tag{4}$$

Now, (3) can be written as follows, to emphasize the relationship between decision threshold and prescribed false-alarm probability:

$$\sum_{i=0}^{\lfloor\tau\rfloor} \left[\binom{\sum_{n=1}^{N} I_n}{i} p_0^i (1-p_0)^{\sum_{n=1}^{N} I_n - i} \right] = 1 - \alpha. \tag{5}$$

According to this equation, the value of threshold τ depends on $\boldsymbol{\alpha}$, $\mathbf{I_n}$ and $\mathbf{N}$. While I_n represents for user's behavior, N represents a trade-off between the detection delay and the threshold accuracy.

In short, the drawbacks of this test are (1) its dependence on the user behavior; (2) its complexity to compute the decision threshold τ and (3) its trade-off between delay and accuracy. If this detector is used, it must be redesigned for each interface of each router, based on the user's behavior and each interface's requirement for delay and accuracy. Such detection scheme has a limited scalability since it needs time and carefulness to be well deployed in the network. Hence, changing the approach is necessary in order to achieve a more scalable detector.

2) Approximation approach: Having solved the exact detection problem with a composite-hypotheses scenario, a simplification is required to achieve a test that can be implemented more easily while preserving the efficiency. Let us start by noticing that, first, each Interest is an independent Bernoulli trial and follows the same distribution with finite variance $var\ =\ p_0(1-p_0)$. Secondly, our hypotheses are related to D_n - the sum of these independent trials. Finally, as in most hypothesis testing problems, the input for the statistical test is a large amount of I_n and D_n's empirical observations. These statements lead us to study the application of the *Central Limit Theorem* (CLT) [14] to transform these hypotheses. By applying the CLT to $\mathcal{H}_0$, one yields:

$$P(\frac{D_n - I_n.p_0}{\sqrt{I_n\ p_0(1-p_0)}} < y)\ \rightsquigarrow\ \Phi(y), \tag{6}$$

Now $\mathcal{H}_0$ will be used to normalize the hypotheses. Let us assign $X_n\ =\ \frac{D_n - I_n.p_0}{\sqrt{I_n\ p_0(1-p_0)}}$. Equation (6) becomes:

$$\begin{aligned} & X_n & \sim\ & N(0,\ 1) \\ \Rightarrow\quad & D_n & \sim\ & N(I_n.p_0,\ I_n\ p_0(1-p_0)). \end{aligned} \tag{7}$$

Applying the CLT to $\mathcal{H}_1$, and then normalize the result following the assigned statistic X_n, we obtain:

$$\begin{aligned} & \frac{D_n - I_n.p}{\sqrt{I_n\ p(1-p)}} & \sim\ & N(0,\ 1) \\ \Rightarrow\quad & D_n & \sim\ & N(I_n.p,\ I_n\ p(1-p)) \\ \Rightarrow\quad & X_n & \sim\ & N(\mu_1, \sigma_1^2), \end{aligned} \tag{8}$$

with

$$\mu_1 = \frac{\sqrt{I_n}.(p\ -\ p_0)}{\sqrt{p_0(1-p_0)}};\ \sigma_1^2 = \frac{p}{p_0}.\frac{1-p}{1-p_0}. \tag{9}$$

Transforming in the opposite way - normalizing the hypotheses under $\mathcal{H}_1$ by assigning $X_n\ =\ \frac{D_n - I_n.p}{\sqrt{I_n\ p(1-p)}}$ - is not relevant. In this way, in order to compute the statistic X_n, except measured values of I_n and D_n, p also must be known in prior. This is impossible since p depends on the attacker's behavior and there is no way to measure it in prior. If we already know p, we already know that an attack is going on and hence there is nothing left to detect.

Now, the addressed hypothesis testing problem becomes:

- $\mathcal{H}_0\ \{p = p_0\} : X_n\ \sim\ N(0,\ 1)$;
- $\mathcal{H}_1\ \{p < p_0\} : X_n\ \sim\ N(\mu_1,\ \sigma_1^2)$,

where $X_n\ =\ \dfrac{D_n - I_n.p_0}{\sqrt{I_n\ p_0(1-p_0)}}$.

The transformed Likelihood Ratio of this test is:

$$(\sigma_1^2\ -\ 1)\sum_{i=1}^{N} X_i^2\ +\ 2\mu_1 \sum_{i=1}^{N} X_i \tag{10}$$

The UMP test barely exists in reality. However, there exists an UMP test if the LR is monotone [14]. Hence it is crucial to study the conditions under which the LR of new hypotheses is monotone. It can be proved that the LR (10) is strictly monotone if:

$$1 - p - p_0\ \neq\ 0. \tag{11}$$

Condition (11) allows us to come up with the following UMP test for the transformed hypotheses:

$$\tilde{\delta}(X_1,\ldots,X_N) = \begin{cases} \mathcal{H}_0 & \text{if } \sum_{i=1}^{N} X_i \geq \tau, \\ \mathcal{H}_1 & \text{if } \sum_{i=1}^{N} X_i < \tau. \end{cases} \quad (12)$$

The threshold τ and the detection power β is determined by the following equations:

$$\tau = \Phi^{-1}(\alpha)\sqrt{N}, \quad (13)$$

$$\beta = \Phi\left(\frac{\Phi^{-1}(\alpha)\sqrt{N} - N\mu_1}{\sigma_1\sqrt{N}}\right). \quad (14)$$

These equation show the main difference between our approach and the mere threshold-based ones. The latter starts by choosing a threshold and then evaluate the PFA and power function by empirical results. To find the best threshold, we have to adjust it and observe the change of PFA and power function. Meanwhile, in our approach, we start with a prescribed PFA value α and calculate the threshold τ based on it. We know exactly how the power function β will change when we modify the PFA value as well as other parameters (e.g. sample size N). The empirical values is to validate the relevance of our theoretical result.

According to (13), the threshold τ of this test only depends on $\boldsymbol{\alpha}$ and $\boldsymbol{N}$. This test has two advantages over the previous one. Firstly, the threshold's calculation is simple and thus low resources-consuming. The accuracy of τ can be improved by gathering more samples in a longer period of time while resources consumption is still unchanged. Again, changing N represents a trade-off between delay and accuracy, but this approach allows establishing a simple relation for this trade-off. Secondly, the detection scheme no longer depends on the user's behavior. A router can use globally configured or manually configured values of α and N. Thanks to these two advantages, this proposed detection method ensures low resources consumption and high scalability.

IV. Evaluation

In our evaluation, we use ndnSIM to simulate data and then run our detection method in MATLAB. The result is compared with the performance of satisfaction-ratio-based detector. This detection method is used in three over four solutions that we presented in Section II-B [11, 12, 13]. We evaluate our detector regarding: (1) relevance of the approach; (2) probabilities of false alarm and detection power as a function of threshold τ; (3) performance in comparison with satisfaction ratio test; (4) detection power in challenging cases.

A. Simulation setup

We used ndnSIM - an open source NS-3 based simulator - to generate data for our evaluation. This simulator faithfully implements the basic components of a CCN network in a modular way [5], which allows us to consider every aspect of the network in the future work. Besides, in order to compare the performance of our approach to the existing one, we reuse one of the topologies in [13] - a binary tree with 8 hosts, intermediate routers and one content provider (as depicted in Figure 2) - for our evaluation. The topology represents one of the worst cases to defend against Interest flooding attack in reality since all the Interests will be forwarded toward upper links and the content provider.

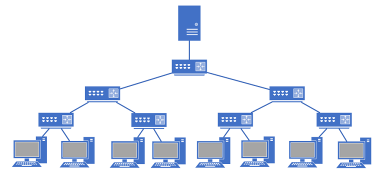


Fig. 2. ndnSIM test scenario

In this topology, the capacity of links and content provider are set up large enough as described in Section III-B. We generate randomly a set of parameters $\{p_0,\ \lambda,\ a\}$ for each host, following these configurations:

- $p_0 \sim unif\ (0,75, 0,85)$: a legitimate user does not send Interests for existent contents all the time, sometimes he makes mistakes. Therefore, the value of p_0 must not be perfect and not too low. As a result, p_0 is chosen randomly in a range of $[0.75, 0.85]$;
- $\lambda \sim unif\ (200, 600)\ packets/second$: since the capacity of links and content provider are assumed to be sufficient in our scenario, choosing a large value for λ is unnecessary. In addition, running simulations with large values of λ is time-consuming while the results are not much different;
- $a \sim unif\ (6, 12)\ packets/second$: instead of sending a large amount of malicious Interests to make routers and content provider go down quickly, an attacker can send a small amount of Interests over time, eventually take up memory space in the PIT. Such attack will require more time to overload routers, but will be more sophisticated and much harder to detect.

Since the addressed Interest flooding is a type DoS attack, there is only one compromised host in each scenario. Each host will become an attacker, alternately. For each scenario, the simulation is run 10 times under each hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$. The generated parameters of each host remain constant for all runs. Finally, 500 seconds are simulated in each run with one sample measured every second. This set up is for gathering a large enough amount of data for post-processing in MATLAB. The simulation code of [13] is re-used as a source code and is modified to integrate all the configurations that we described. Our evaluation results is demonstrated in the following subsection.

B. Evalution results

1) Relevance of approach: Figure 3 shows that although a host's histograms of UMP statistics (X_n) varies widely under both $\mathcal{H}_0$ and $\mathcal{H}_1$, their empirical distributions perfectly match the theoretically established probability distribution functions, see (8) and (9). The distributions of UMP test

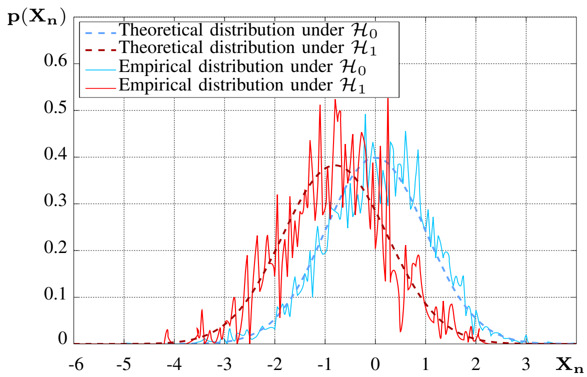


Fig. 3. Comparison between empirical and theoretical distribution of UMP test results for one host under both $\mathcal{H}_0$ (right side) and $\mathcal{H}_1$ (left side).

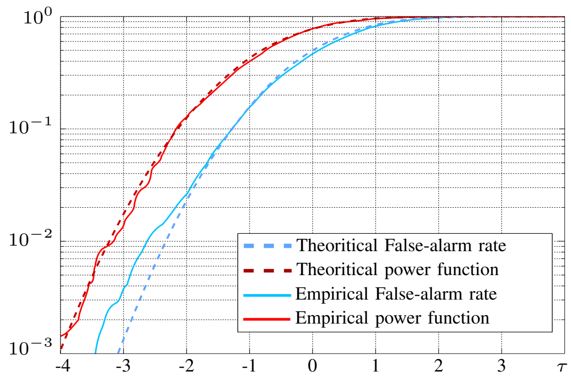


Fig. 4. Comparison between the theoretical and empirical for both false alarm probability and detection power as a function of decision threshold τ.

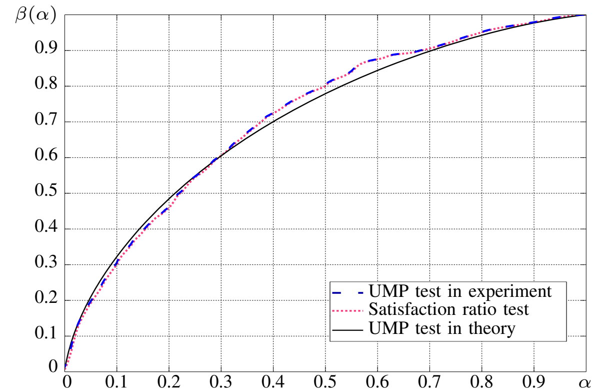


Fig. 5. Comparison between the proposed UMP test and the satisfaction ratio test for a single host with fixed traffic properties.

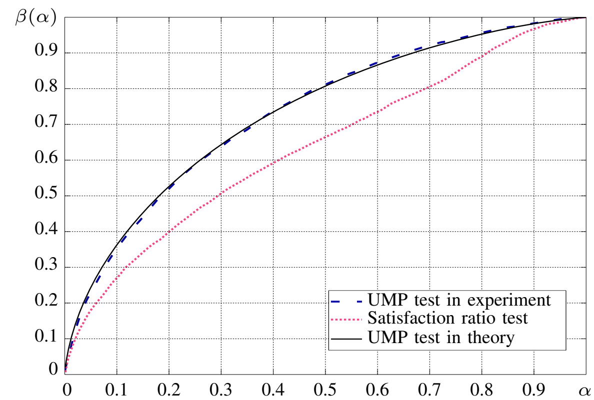


Fig. 6. Comparison between the proposed UMP test and the satisfaction ratio test for several nodes which have different traffic properties.

statistics from other nodes also provide us with the same conclusion, implying that transforming the original hypotheses with CLT approximation is a very relevant approach for the addressed problem.

2) Probabilities of false alarm and detection power as function of τ: Figure 4 depicts the change of PFA and detection power as function of threshold τ. When τ is modified, the empirical values of detection power and PFA are close to the theoretical ones, implying that no matter what τ is, both detection power and PFA of our detection method are always under control. In other words, when τ needs to be modified, one knows exactly how the proposed detector will change. Meanwhile, none of the existent solutions have studied this problem yet and hence, their performance remains formally unknown.

3) Performance in comparison with satisfaction ratio test: Figure 5 and Figure 6 present the *Receiver Operating Characteristic* (ROC) curve of our UMP test and satisfaction ratio test with fixed traffic properties for a single host and all nodes, respectively. A ROC curve illustrates the performance of a test by showing the variation of detection power as a function of PFA. A good statistical test will have a ROC curve which reaches the top-left corner of the graph. Such curve demonstrate a statistical test with high power and low false alarm probability.

Figure 5 shows a comparison between performances of the satisfaction ratio detector and the proposed UMP test for a single host. Although the empirical ROC curve of our UMP test for a single host precisely matches the theoretical one, the satisfaction ratio test also achieves the same performance. However, the latter has not been studied statistically and the condition under which it is optimal has never been identified as well as its statistical performance.

However, if we draw the ROC curve for an overall performance (as depicted in Figure 6) by concatenating all simulated data from all nodes which have different traffic properties, the difference is now revealed. The proposed UMP test's performance not only perfectly matches the theoretical one, but also shows a much better performance than the satisfaction ratio test.

4) Detection power in challenging cases: Figure 7 depicts the empirical and the theoretical *Probability of Missed Detection* (PMD) of our UMP test as a function of hit rate under attack p with fixed values $\alpha = 0.05$, $N = 1$ and $p_0 = 0.85$. The PMD is is the probability that $\mathcal{H}_1$ is rejected when it is actually true. In other words, $PMD = 1 - \beta$. A graph of PMD is used to better illustrate the result of this evaluation and to improve the readability.

As demonstrated in the Figure 7, the empirical power of our test perfectly matches the theoretical one, proving that

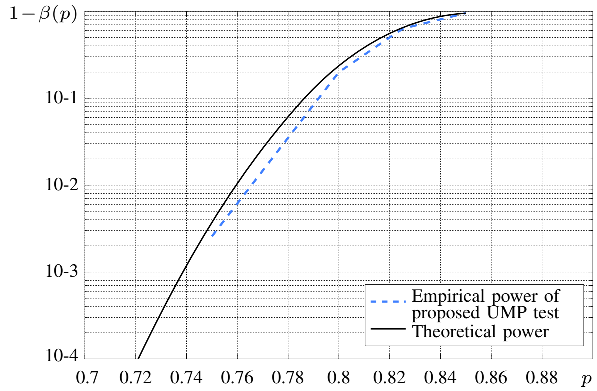


Fig. 7. Comparison between the empirical and the theoretical PMD of the proposed UMP test, for a single host, as a function of p. Here $\alpha = 0.05$ and $p_0 = 0.85$.

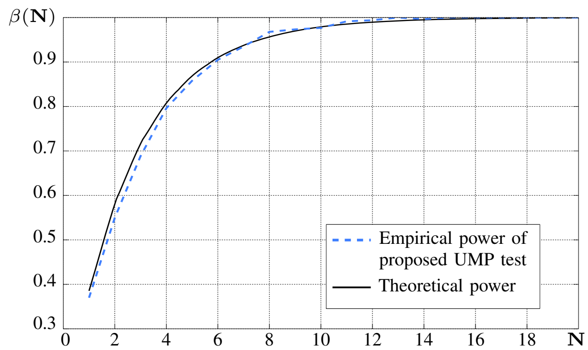


Fig. 8. Comparison between the empirical and the theoretical power of the proposed UMP as a function N. Here $\alpha = 0.05$, $p = 0.85$ and $p_0 = 0.825$.

our detector is well established and results deduced from this figure are reliable. The figure emphasizes that the proposed UMP test achieves very low PMD for most values of p. If the attacker wants to defeat the proposed UMP test, he is limited to an attack with a very small amount of malicious Interests (p is very close to p_0). Such attack requires more time to overload routers and content providers.

Empirical results for attacks with large amount of malicious Interests ($p < 0.75$) are also simulated. Since the detection power for those cases is nearly perfect (i.e. $PMD \approx 0$), those results cannot be demonstrated in the logarithm scale of the figure.

Figure 8 demonstrates the detection power of our UMP test as a function of sample size N with fixed values $\alpha = 0.05$, $p_0 = 0.85$ and $p = 0.825$. First, this figure presents the trade-off between accuracy and detection delay through sample size N in the most visual way. Secondly, our empirical result is perfectly compatible with the theoretical one, implying that our detector is well established and the results deduced from this figure are reliable.

This configuration represents a challenging case for our proposed detector since the attacker's and the legitimate user's traffic are very similar to each other. As depicted in Figure 7, this attack causes a high PMD to our optimal statistical test. However, it also requires more time to overload routers and content providers, offering our detector more time to gather samples in order to enhance the detection power against this attack. In short, our proposed UMP test has an advantage over Interest flooding attack, even when the attack is launched with a small amount of malicious Interests.

With all of the previously presented numerical results, we come to the following conclusions. Firstly, CLT approximation is a very relevant approach for our problem. Secondly, we can master the detection power and the PFA of our UMP test. Thirdly, our proposed detection method has a better overall performance than the satisfaction ratio test. Fourthly, the optimal statistical test provides a great power in most values of p. In addition, attackers are limited to attacks with a very small amount of malicious Interests. Finally, thanks to the analytically established statistical performance of the proposed detector, one can select a balance point for the trade-off between accuracy and delay for the proposed UMP test. Moreover, our proposed UMP test has an advantage over Interest flooding attack, even when the attack is performed with a small amount of mischievous Interests.

V. Conclusion

Using statistical hypothesis testing theory, we achieved the required detection method for our problem and the result is promising. The proposed detector is simple enough to be deployed on every interface of all routers. Its threshold does not depends users' behavior on each interface and can be globally or manually configured. We performed simulations in ndnSIM to evaluate the performance of the optimal statistical test and compare it to existent satisfaction ratio test. The optimal statistical test provides a better overall performance than the satisfaction ratio test and the observed empirical results perfectly matches the theoretically established one thanks to a thorough statistical analysis. Furthermore, even though the Interest flooding attack is launched with a very small amount of bad Interests, our proposed detector always gain an upper hand over the attack.

However, there are some limitations that we want to improve in our future work. First, we need to actually integrate the proposed detector in a CCN implementation. Secondly, in order to truly evaluate the scalability and the resource consumption, our proposal must be experimented on more topologies with consideration to other factors. Thirdly, a mitigation strategy after the detection phase should be developed to actually neutralize the attacker. Finally, we will address a more clever attack in which the attacker's behavior as well as the hit ratio under normal case change over time.

Acknowledgment

This work is partially funded by the French National Research Agency (ANR), DOCTOR project <ANR-14- CE28-000> and supported by the French Systematic ICT cluster.

References

[1] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of Information-Centric Networking," *Communications Magazine, IEEE*, vol. 50, no. 7, pp. 26–36, 2012.

[2] G. Xylomenos, C. Ververidis, V. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K. Katsaros, and G. Polyzos, "A survey of Information-Centric Networking research," 2013.

[3] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "DoS and DDoS in Named Data Networking," in *Computer Communications and Networks (ICCCN), 2013 22nd International Conference on*. IEEE, 2013, pp. 1–7.

[4] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking Named Content," in *Proceedings of the 5th international conference on Emerging networking experiments and technologies*. ACM, 2009, pp. 1–12.

[5] A. Afanasyev, I. Moiseenko, L. Zhang *et al.*, "ndnSIM: NDN simulator for ns-3," *University of California, Los Angeles, Tech. Rep*, 2012.

[6] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica, "A data-oriented (and beyond) network architecture," *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 4, pp. 181–192, 2007.

[7] S. Tarkoma, M. Ain, and K. Visala, "The publish/subscribe internet routing paradigm (PSIRP): Designing the Future Internet architecture." in *Future Internet Assembly*, 2009, pp. 102–111.

[8] C. Dannewitz, D. Kutscher, B. Ohlman, S. Farrell, B. Ahlgren, and H. Karl, "Network of information (NetInf) - an Information-Centric Networking architecture," *Computer Communications*, vol. 36, no. 7, pp. 721–735, 2013.

[9] H. Dai, Y. Wang, J. Fan, and B. Liu, "Mitigate DDoS attacks in NDN by interest traceback," in *Proc. of IEEE INFOCOM, NOMEN Workshop*, 2013.

[10] T. Lauinger, "Security & scalability of Content-Centric Networking," Master's thesis, TU Darmstadt, the Netherlands, 2010.

[11] J. Tang, Z. Zhang, Y. Liu, and H. Zhang, "Identifying Interest flooding in Named Data Networking," in *Green Computing and Communications (GreenCom),IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing*. IEEE, 2013, pp. 306–310.

[12] A. Compagno, M. Conti, P. Gasti, and G. Tsudik, "Poseidon: Mitigating Interest flooding DDoS attacks in Named Data Networking," in *IEEE Conference on Local Computer Networks (LCN)*. IEEE, 2013, pp. 630–638.

[13] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, "Interest flooding attack and countermeasures in Named Data Networking," in *IFIP Networking Conference, 2013*. IEEE, 2013, pp. 1–9.

[14] E. L. Lehmann and J. P. Romano, *Testing statistical hypotheses*. Springer, 2006.

[15] V. S. Frost and B. Melamed, "Traffic modeling for telecommunications networks," *Communications Magazine, IEEE*, vol. 32, no. 3, pp. 70–81, 1994.

[16] D. Goergen, T. Cholez and J. François and T. Engel, "A semantic firewall for Content-Centric Networking," in *Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium*. IEEE, 2013, pp. 478–484.

[17] S.U. Khan, T. Cholez, T. Engel and L. Lavagno, "A key management scheme for Content Centric Networking," in *Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on*. IEEE, 2013, pp. 828–831.