Economic Levers for Mitigating Interest Flooding Attack in Named Data Networking

Hindawi
Mathematical Problems in Engineering
Volume 2017, Article ID 4541975, 12 pages
https://doi.org/10.1155/2017/4541975

Research Article

Economic Levers for Mitigating Interest Flooding Attack in Named Data Networking

Licheng Wang,[1] Yun Pan,[2] Mianxiong Dong,[3] Yafang Yu,[4] and Kun Wang[2]

[1]*State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2]*School of Computer Sciences and Technology, Communication University of China, Beijing 100024, China*
[3]*Department of Information and Electronic Engineering, Muroran Institute of Technology, 27-1 Mizumoto-cho, Muroran, Hokkaido 050-8585, Japan*
[4]*Anyang Normal University, Anyang, Henan 455002, China*

Correspondence should be addressed to Licheng Wang; wanglc2012@126.com

Received 14 February 2017; Accepted 18 April 2017; Published 7 June 2017

Academic Editor: Zonghua Zhang

As a kind of unwelcome, unavoidable, and malicious behavior, distributed denial of service (DDoS) is an ongoing issue in today's Internet as well as in some newly conceived future Internet architectures. Recently, a first step was made towards assessing DDoS attacks in Named Data Networking (NDN)—one of the promising Internet architectures in the upcoming big data era. Among them, interest flooding attack (IFA) becomes one of the main serious problems. Enlightened by the extensive study on the possibility of mitigating DDoS in today's Internet by employing micropayments, in this paper we address the possibility of introducing economic levers, say, dynamic pricing mechanism, and so forth, for regulating IFA in NDN.

1. Introduction

Today's Internet is a unique and unprecedented global success story [1]. It is built based on TCP/IP architecture and assumes that users and ends are trustable and intelligent, and the main task of the Internet is to provide best effort service of packet forwarding. This idea caters to the original requirements on mutually connecting hosts and sharing distributed resources. However, with the increasing and flourishing of the models of computations and applications, the way people access and utilize the Internet has changed dramatically, and today's Internet is reaching the limits of their senescence [1]. To keep pace with changes and move the Internet into the future, several projects have been initiated to design potential next-generation Internet architectures [1].

In 1999, Adjie-Winoto et al. [2] proposed the concept of "Content-Centric." Afterwards, more researchers have been paying efforts on this direction, and the idea of Information Centric Networking (ICN) is widely accepted, now. With ICN, each piece of information has a unique name as its identity, by which users can request consuming desired information, while the network needs only to manage the flowing and cache these pieces of information according users requests and information's names. In other words, with ICN, users need only to know what he/she wants, instead of where the information is located. Names themselves carry less information about routing than IP addresses used in today's Internet. Recently, big ICN research projects are mainly distributed in Europe and America, such as Date-Oriented Transfer (DOT) architecture [3], Data-Oriented Network Architecture (DONA) [4], Routing on Flat Labels (ROFL) [5], Internet Indirect Infrastructure (or i3 for short) [6], Publish-Subscribe Internet Routing Paradigm (PSIRP) [7], Content-Centric Networking (CCN) [8–10], 4WARD [11], and TRIAD [1]. Among them, Content-Centric Networking (CCN) due to Jacobson et al. [8–10] is currently a comparatively mature architecture. In particular, CCN*x* [10] is an open-source suite that enables more researchers to put forward their improvements as well as CCN-based new applications [12]. In recent years, the project Named Data Networking (NDN) [13],

with thoroughly integrating the idea of ICN/CCN, made remarkable progress, including a series of typical applications [14, 15], as well as NS-3 friendly simulation tools for further development [16]. In particular, in the upcoming big data era, NDN will inevitably become one of the promising Internet architectures due to is data-centric features.

In order to avoid past pitfalls, security experts insist that we should treat security and privacy as fundamental requirements, and in particular resilience to denial of service (DoS) and distributed denial of service (DDoS) attacks become a major issue and deserve full attention during conceiving next-generation Internet architectures [1]. Recently, Gasti et al. [1] made a first step towards assessing DDoS attacks in NDN. On one hand, many kinds of DoS/DDoS attacks that have heavy impact on today's Internet are successfully bypassed due to subtleties and exactitude of designing of NDN. In particular, the pulling model and the receiver-driven mechanism used in NDN make most DoS/DDoS attacks becoming aimless (i.e., it is difficult to find victims), and the mechanism of reverse path content delivering makes most DoS/DDoS attacks reflect to themselves. But as the proverb goes, "every coin has its two sides," NDN has not uprooted DoS/DDoS attacks. Gasti et al. also conceived two kinds of new DoS/DDoS attacks that intentionally utilize the features of NDN: interest flooding attack (IFA) and content/cache poisonous attack (CPA). Shortly afterwards, Atanasyev et al. [17] showed that NDN's inherent property of flow balancing provides the basis for effectively mitigating IFA.

However, as far as we know, little attention is paid to mitigating IFA in NDN by employing micropayment systems. But we know that in fighting against DoS/DDoS attacks on today's Internet, micropayments have been extensively studied during the past two decades [18]. The idea of micropayments in fighting against DoS/DDoS attacks focuses on incurring heavy penalties such as "virtual money" (say, CPU cycles, memory/disk, bandwidth, etc.) to the DoS/DDoS attackers. Therefore, in this paper, we try to probe the possibility of using economic levers, such as micropayments and different pricing functions, to deal with the interest flooding attacks in NDN. Our discussion mainly includes three parts: a prototype of economic model for NDN, evaluation on knowing types of micropayments in NDN, and assessing the possible utilities of knowing pricing functions in NDN. In addition, we also address the possibility of charging content producers and relate this issue to the area of digital right management (DRM).

The rest of content is organized as follows: in Section 2, we give a brief introduction on NDN and IFA; in Section 3, our main contribution, a prototype of economic model for NDN, is proposed; finally, the concluding remarks are found in Section 5.

2. Reviewing NDN and Interest Flooding Attacks

As a typical instance of the broader ICN/CCN approach to networking, NDN aims to evolve it into an architectural framework for the future Internet [1]. NDN eliminates host-based addressing and explicitly names content and thus transforms content into a first-class entity [17]. Based on this abstraction there is no explicit notion of "hosts" in NDN, although their existence is assumed. Instead, interest and content are the only two types of packets in NDN, and each NDN router maintains three major data structures [1]:

(i) Pending Interest Table (PIT), a table containing currently unsatisfied interests and corresponding incoming interfaces

(ii) Forwarding Interest Base (FIB), a table containing name prefixes and corresponding outgoing interfaces

(iii) Content Store (CS), a buffer used for content caching and retrieval

Based on these components, communication in NDN takes the *pull* model: A consumer requests content by sending an interest packet; if an entity (a router or a host) can fetch from his CS a matched content object (i.e., named data packet), the corresponding data packet will be returned to the consumer by following the reverse path of the interest request [17]. These features make NDN a receiver-driven, data-centric communication protocol [17] and thus automatically bypass several long-standing DoS/DDoS attacks, such as direct flooding and reflector attacks through source address spoofing [17].

However, in 2012, Gasti et al. conceived the so-called interest flooding attacks (IFA) that utilize the features of NDN: the adversary, with controlling of a large set of zombies, invokes a large number of interest requests that are distributed closely in space, aiming to overflow PITs in routers, preventing them from handling legitimate interests, and/or to swamp the specific content producer(s) [1]. Gasti et al. further identified three types of IFA based on the whether the requested content exists and how the content produced [1]:

(I) Existing and static

(II) Dynamically generated

(III) Nonexistent

As for IFA with type (I), the impact on NDN routers is limited since in-network content caching mechanism will automatically block subsequent same/similar interest requests not to propagate to the producer(s). As for IFA with type (II), the impact on NDN routers varies with respect to their distance from the targeted content producer(s): the closer the router to the producer(s), the greater the effect on its PIT [1]. IFA with type (III) cannot incur significant overhead for targeted content producer(s), but unsatisfied interest requests will propagate to other NDN nodes and the corresponding PIT entries will be occupied with longest time—until they eventually expire [1].

3. A Prototype of Economic Model for NDN

It is a common belief that a resource may be abused if its users incur little or no cost [19]. Thus, it is reasonable to introduce payments or in general micropayments into NDN for fighting IFA. In fact, the idea of requiring the user to commit its resources before requesting services was described early by

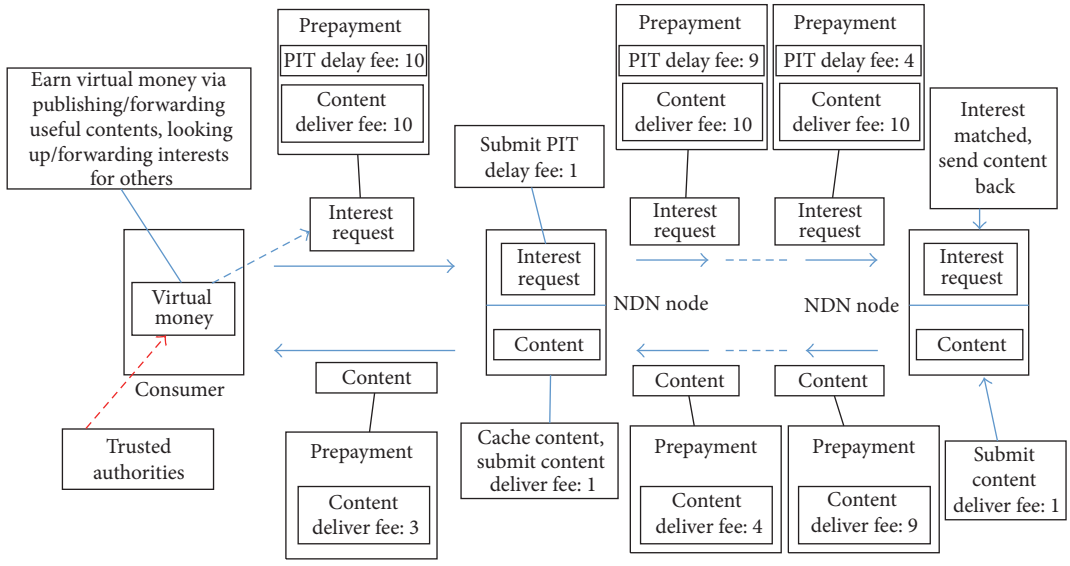


Figure 1: The proposed prototype of economic model for NDN.

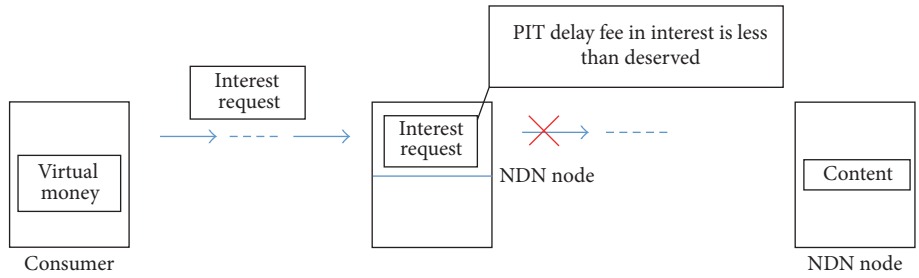


Figure 2: Dropping interest request due to lack of PIT delay fee.

Dwork and Naor [20, 21]. As early as about 10 years ago, Mankins et al. [18] once introduced dynamic resource pricing models for mitigating distributed denial of service attacks. But their models were conceived under the scenarios with typical TCP/IP architectures, and thus some aspects need to be updated for NDN architecture accordingly.

3.1. Business Logics. For mitigating IFA in NDN, the proposed prototype of economic model is featured by the following business logics:

(1) Suppose that there are trusted authorities in NDN, and they do not only play the role of central banks for issuing virtual money (VM) and related strategies, but also conduct related tasks like auditing, accounting, and so on (as analogy of reality, one might prefer to assign the duties of auditing and accounting to other trusted authorities, instead of banks; but this has no essential effects on our prototype).

(2) Suppose each user or NDN node possesses certain amount of VM at the beginning, and he/she can earn more VM via publishing/forwarding useful contents, looking up/forwarding interests for others.

(3) Each user is required to submit his/her prepayment (PP), as long as prompting an interest request. This prepayment includes two parts: PIT delay fee (PDF) and content delivering fee (CDF).

(4) Upon receiving an interest request from some downstreaming node that might be an end consumer or a NDN router the NDN node i looks up his/her local cache for interest matching: if failing, then make allowance for PIT delay fee, denoted by pdf_i, and then forward the interest request to all/part of upstreaming nodes; if matched, then make allowance for content delivering fee, denoted by cdf_i, and then transfer the content to the requester via a reverse path along the interest request; and every NDN node j in this path will also make allowance for content delivering fee cdf_j and meanwhile keep the content in his/her local cache (see Figure 1).

(5) Each NDN node can stop and discard interests forwarding if the left prepayment carried by the request package is less than his/her charging on PIT delay fee (see Figure 2). Similarly, each NDN node can stop contents forwarding (i.e., the red crossing

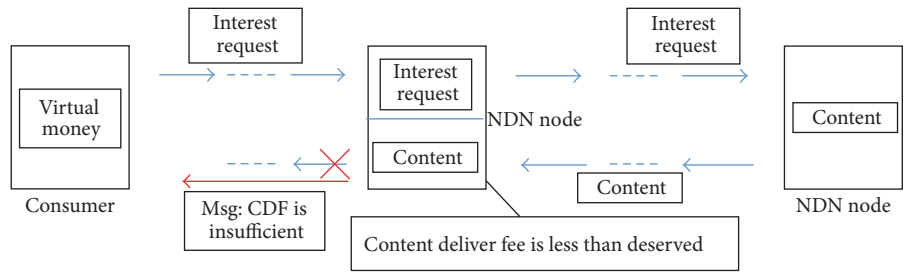


Figure 3: Stopping content delivering due to lack of prepayments.

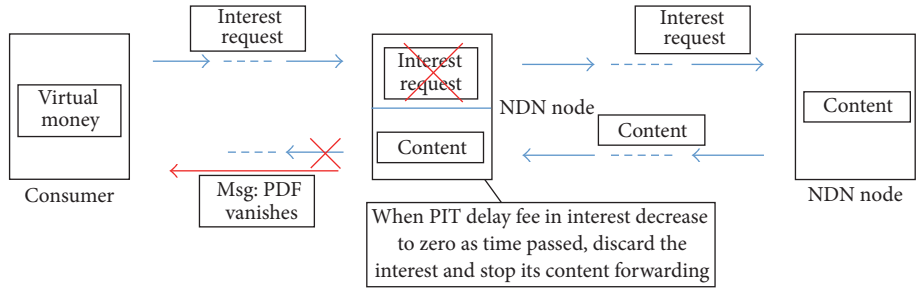


Figure 4: Stopping content delivering due to PIT delay fee vanishes.

symbol in Figure 3) if the left prepayment is less than his/her charging on content delivering fee. This is reasonable since the forward node, as well as the downstream nodes, has no obligation to delivering packages without earnings. However, this node need not immediately discard this kind of undelivered content. Instead, he/she can choose to cache this content for short period and meanwhile send a short message "CDF is insufficient" to the requester via a reverse path along the interest request. This kind of short message can be regarded as special "contents" packets and the related content delivering fee is set to zero.

(6) PIT delay fee vanishes with its delay time in PIT table. In other words, as for some item in a PIT table, its PIT delay fee pdf_i will decrease along time elapse, and the NDN node will discard this PIT item if this $\text{pdf}_i \leq 0$. When this occurs, the NDN node can also send another short message "PDF vanishes" to the requester via a reverse path along the interest request. Similarly, this kind of short message can also be regarded as special "contents" packets and the related content delivering fee is set to zero. Meanwhile, the two red crosses in Figure 4 indicate that the related forwarding processes are also cancelled. This is reasonable considering that some nodes might become unreachable after he/she sends requests. In this case, it is useful to space the PIT buffers for accommodate newly coming requests.

(7) All involved economic behavior should be auditable and accountable. Enforcing each NDN node to sign his/her actions or responses related to VM provides a good support for achieving postauditing and accounting. Auditing and accounting should be executed by some trusted authorities periodically.

Remark 1. Compared to the original NDN architecture, the processes of delivering the above two kinds of short messages are newly introduced. Based on the following observations, we think these new additions are compatible with the original NDN architecture and useful for improvement the performance.

(i) If a NDN router node directly discards related PIT entries in local PIT table but without sending the short message "CDF is insufficient" or the short message "PDF vanishes" then we return to the original NDN settings.

(ii) Upon receiving either of these two special messages, an end user can choose to resend the same interest request with additional prepayments. Then, the interested contents might be fetched quickly in the midway.

(iii) Since these two short messages are transferred along the reverse path of interest requests, the downstreaming NDN nodes can take actions correspondingly:

(a) If the corresponding PIT entry still stays in local PIT table, then the NDN node can forward the incoming short messages downwards and then discard this PIT entry.

(b) Otherwise, if the corresponding PIT entry has already been discarded from local PIT table, then the NDN node no longer need forward the incoming short messages downwards, since before this occurs, it might have sent the short

message "PDF vanishes" along the reverse of the path of interest requests. Recursively, the related end users have the chance to receive at least one short message and this is sufficient for prompting him/her to resend the same interest request with additional payments.

Remark 2. Someone might argue whether the business logic depicted in Figure 3 is reasonable. Seemingly, it is unfair for the consumer because no service has been provided in this case. Someone is even afraid of the fact that based on this business logic a DoS attack can be mounted by sending interest requests with calculated insufficient CDF. However, we insist that the business logic depicted in Figure 3 is reasonable:

(i) Firstly, it is unfair for NDN routing nodes if in this case the consumer is not charged. Anyway, the involved NDN routing nodes have already done searching on related interests and even transferring contents during the network, although the contents have not reached the consumer. That is, we must pay NDN routing nodes. Without charging consumer, who pays that?

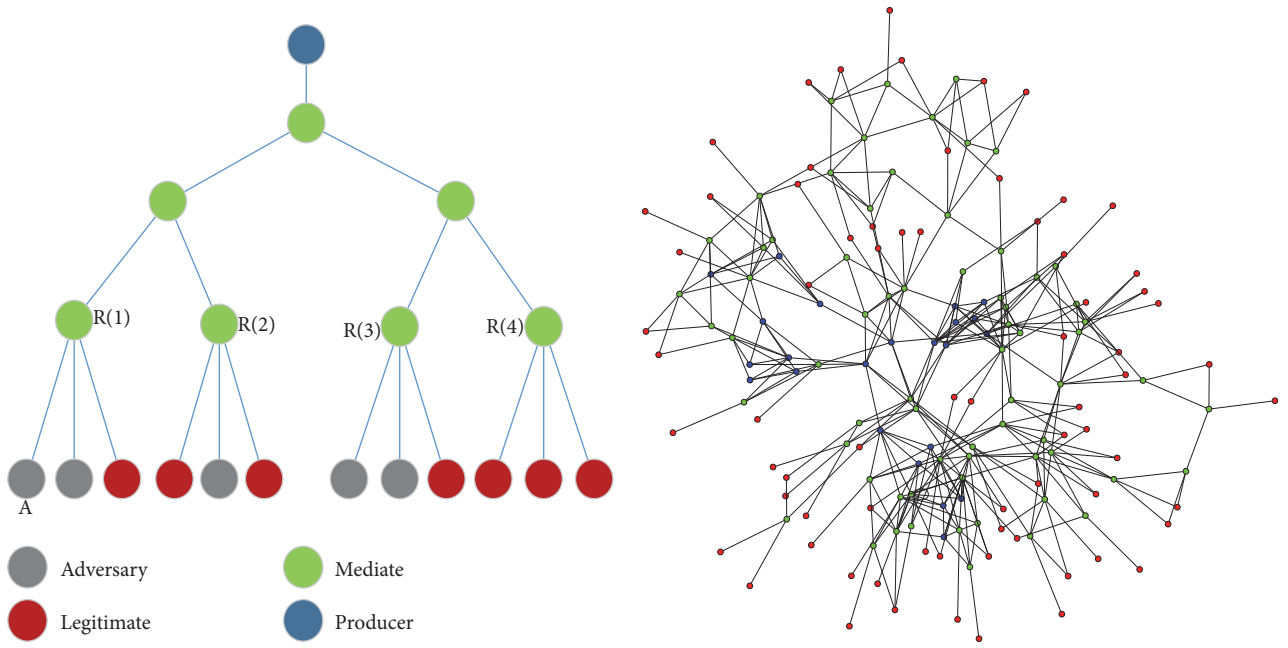
(ii) Secondly, even though the requested contents have not reached the consumer, the consumer obtains a useful message: CDF is insufficient. This message tell two facts to the consumer: (a) the interest request has been matched and (b) the requested content has already been stored in the halfway—this is just the core feature of NDN. That is, the consumer can launch the same interest request and then get the content from the halfway.

(iii) Thirdly, suppose one node, denoted by A, tries to mount a DoS attack by sending interest requests with calculated insufficient CDF. That means the prepayment of A should be large enough for routing NDN nodes find the matched contents; otherwise, the case in Figure 2, instead of the case in Figure 3, occurs. Now, suppose that the content is dropped in the halfway due to lack of CDF. Then, when A launches the same interest request again, also with insufficient CDF, now the request interest must be matched during the halfway. Again and again, the matched contents will come to A closer and closer. That is, the effects of this kind of DoS attack towards the whole network become less and less. Finally, when the content has merely one hop to A, this kind of DoS attack becomes useless.

3.2. Types of Micropayments. As addressed in [18], micropayments can provide a useful side benefit by providing a uniform means of resource accounting, pricing, and arbitration. But micropayments mechanisms must not impose an undue performance penalty. That is, the performance should be, in the absence of an attack, nearly comparable to a system that does not use the payment mechanisms [18]. There have been a number of digital payment and micropayment schemes to support digital exchanges [18, 22]. According to the description of the above prototype, we need fungible (or transferable) digital payment schemes. Among them, check or credit card-like schemes require some type of online verification of payment—a server connects online much with a bank and verifies the creditworthiness of the requester [18]. Apparently, this strategy is not suited for NDN since the server might become easily a bottle neck; cash-like schemes do not require online verification but require significant computation or memory usage overhead for validation [18] and thus may not be compatible with NDN-oriented applications; scrip-based system (such as Compaq's Millicent [23]) is featured in that the verification can be performed locally with very low latency and thus it is friendly to NDN-oriented applications. Note that today's popular digital cash BitCoin [24] might not be suited for NDN-oriented applications considering that it becomes more and more difficult to obtain a "coin"—this suggests that the mechanism of BitCoin does not provide a steady supply of currency with the flourishing of the applications in future. However, moderately hard, memory-bound functions suggested by Abadi et al. [19] might be useful. In particular, this kind of functions is evaluated at about the same speed on most popular systems like severs, laptops, PDAs, and so forth [19]. Recently, Shen et al. [21] suggested using retraffic strategy for fighting against DDoS in TCP/IP architecture. However, this method does not only rely on middle-software that is fixed in front of the server, but also request the client to send more traffic (i.e., retraffic) for a single request. After that, Khanna et al. [25] also proposed using bandwidth as currency. That is, in order to get service, the clients are encouraged to spend more bandwidth by either sending repeated requests or sending dummy bytes on a separate channel to enable a bandwidth auction [25]. However, as for NDN architecture, we state as a fact two obstacles for deploying these two methods: firstly, interest request in NDN is forwarded by NDN router nodes and the upstreaming nodes need not recognize the end client, and thus requesting the interrouter nodes to spend more bandwidth is irrational; secondly, where to deploy the newly introduced middle-software is not only a cost problem, but also an challenge with respect to modifying NDN architecture. Therefore, we are inclined not to use these two methods in NDN. In brief, we summarize the potential NDN compatibilities of different kinds of micropayments in Table 1.

Table 1: Compatibility of micropayments in NDN.

Types	Features/requirements	Compatibilities
Check/credit card-like	Online verification	Poor
Cash-like	Heavy local verification	Poor
Scrip-based	*Light local verification*	*Good* √
BitCoin-like	Lack of supply	Poor
Memory-bound functions	*Roughly same speed over different platforms*	*Good* √
Retraffic or bandwidth as payment	Clients are encouraged to spend more bandwidth	Poor



(a) A tree-like topology

(b) A net-like topology

Figure 5: Topologies for simulation.

3.3. Pricing Functions. It is also another common sense that we should employ a dynamic pricing strategy for each service, instead of a fixed pricing function for all services [18]. However, detailed addressing of this issue goes out the scope of this paper. As the first step towards analyzing possibility of using economic levers in NDN, we would like to abstractly classify all services in NDN into two categories: interest looking up and content delivering. In other words, from the view of NDN router nodes, all interests/contents in the above prototype have no much difference from random numbers. Their duties are just to look up, to forward, and to cache them. After that, these NDN routers will obtain what they deserved (i.e., VM) according certain charging policies. Note that this kind of abstraction does not exclude the following two possibilities: (1) pricing function may be time-varying according to NDN routers' capabilities and other situations of the network, like congestion and so forth; (2) Each end user has their *own* utility function that determines how much he/she is willing to pay for an interest request, although after submitting his/her interest request, all related NDN router nodes will charge PIT delay fee (i.e., pdf) and content delivering fee (i.e., cdf) regardless of which kind of interests/contents is requested/delivered. In fact, in our micropayment system, we can adopt the following price model:

$$\text{Price} = \max\{0, -U(\text{utility}) + C(\text{opportunity cost})\}, \quad (1)$$

where both the utility function U and the opportunity cost (this indicates the potential cost of giving bandwidth to the coming request while not giving to others) function C can be established in an adaptive manner, according to the long term competition and balance between the requests and the responses of NDN network services.

In the scenario of mitigating TCP SYN flooding attacks, Mankins et al. tested four different pricing functions [18]:

(i) Constant function ($p = k$): the price p is set to constant k regardless of its level of consumption.

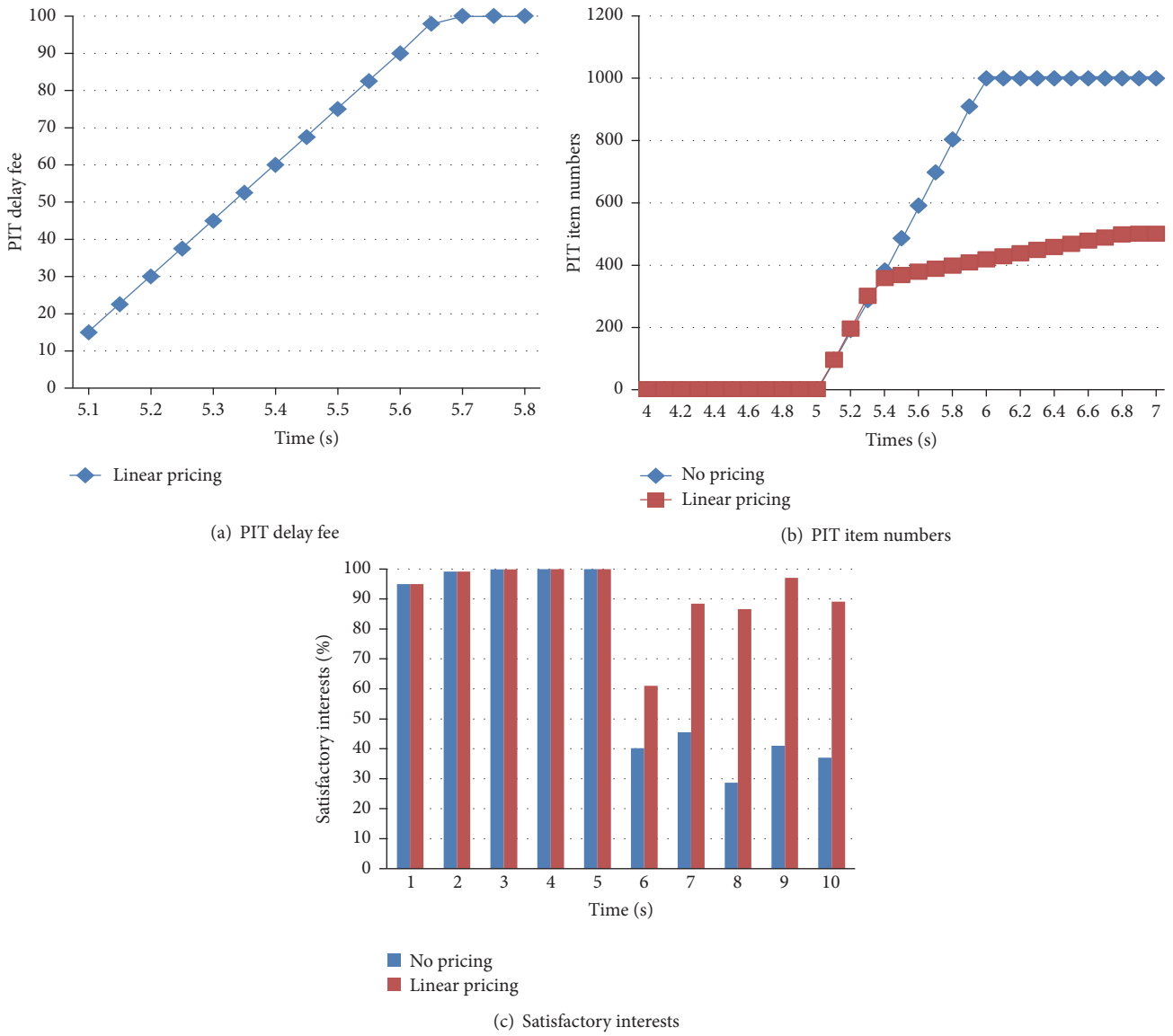
(ii) Linear function ($p = kc$): p is proportional to the value of a chosen market observable c such as the number of current connections.

(iii) Asymptotic function ($p = kB/(B - c)$): p is raised asymptotically to infinity as the market observable c approaches its limitation B.

(iv) Exponential function ($p = \alpha e^{\beta c}$): p is raised in the fastest manner with respect to the increasing value of the market observable c.

In fact, we can see that these pricing functions are reasonable in wide and universal scenarios and they are independent of concrete architectures. For example, the asymptotic pricing strategy is useful in safeguarding a resource with a hard limit in capacity, while the exponential pricing strategy is effective in controlling consumption of a critical resource [18]. The thing left is to consider how to use them, respectively, for mitigating interesting flooding attack in NDN.

(1) *Constant Pricing Function.* With the purpose of providing steady service, it seems that the simplest way is to use constant pricing strategy for forwarding incoming interest requests within the same time-window and with the same local connection degree. However, we think it is not suitable for our scenario: first, NDN architecture is topology-insensitive but constant pricing function should be, at least locally,



(a) PIT delay fee

(b) PIT item numbers

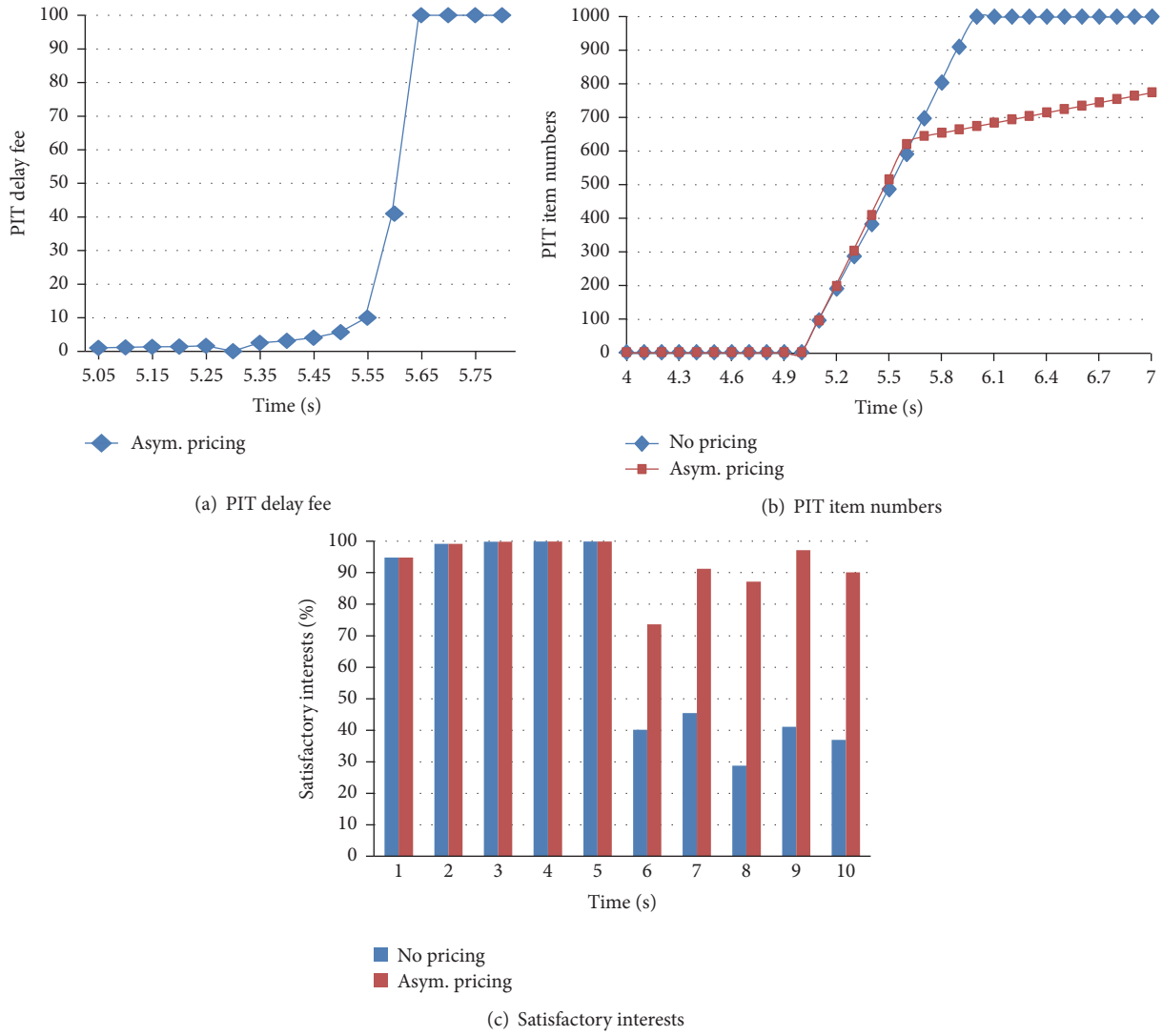
(c) Satisfactory interests

FIGURE 6: Simulation on linear pricing strategy ($k = 0.3$).

topology-aware; second, constant pricing function will charge IFA nodes with an unbiased mind, but our main motivation is to punish IFA nodes and the so-called unbiased mind towards malicious nodes will be *unfair for* legitimate nodes. Therefore, for mitigating IFA attacks, we will *not suggest using* constant pricing function.

(2) *Linear Pricing Function.* Since the concept of connection is not explicitly modeled in NDN architecture, we associate c in the related pricing functions to the number of interest requests coming from some ports. As a result, whenever a malicious node, denoted by $\mathscr{A}$, launches IFA attacks, the numbers of interest requests in PIT tables of $\mathscr{A}$'s upstreaming nodes increase linearly. This in turn induces linear increment of charging $\mathscr{A}$'s prepaid. When it is used out, the related interest request will be discarded. As for legitimate nodes, this kind of accumulation of interest request will not occur in PIT tables of the upstreaming nodes; thus the charge will be much small.

(3) *Asymptotic Pricing Function.* Here, c is also associated with the related pricing functions to the number of interest requests coming from some ports, while B is associated with the maximum number of interest requests that can be accepted by an upstreaming node. We will use asymptotic pricing function for *basically* charging PIT delay fee (i.e., pdf) (here, the term "basically" means the least charging without considering the further delay of PIT entries in PIT tables). That is, when the local PIT table becomes almost occupied, a NDN router node has to charge *hugely* for newly incoming interest requests. By using this



(a) PIT delay fee

(b) PIT item numbers

(c) Satisfactory interests

FIGURE 7: Simulation on asymptotical pricing strategy ($k = 1$, $B = 333$).

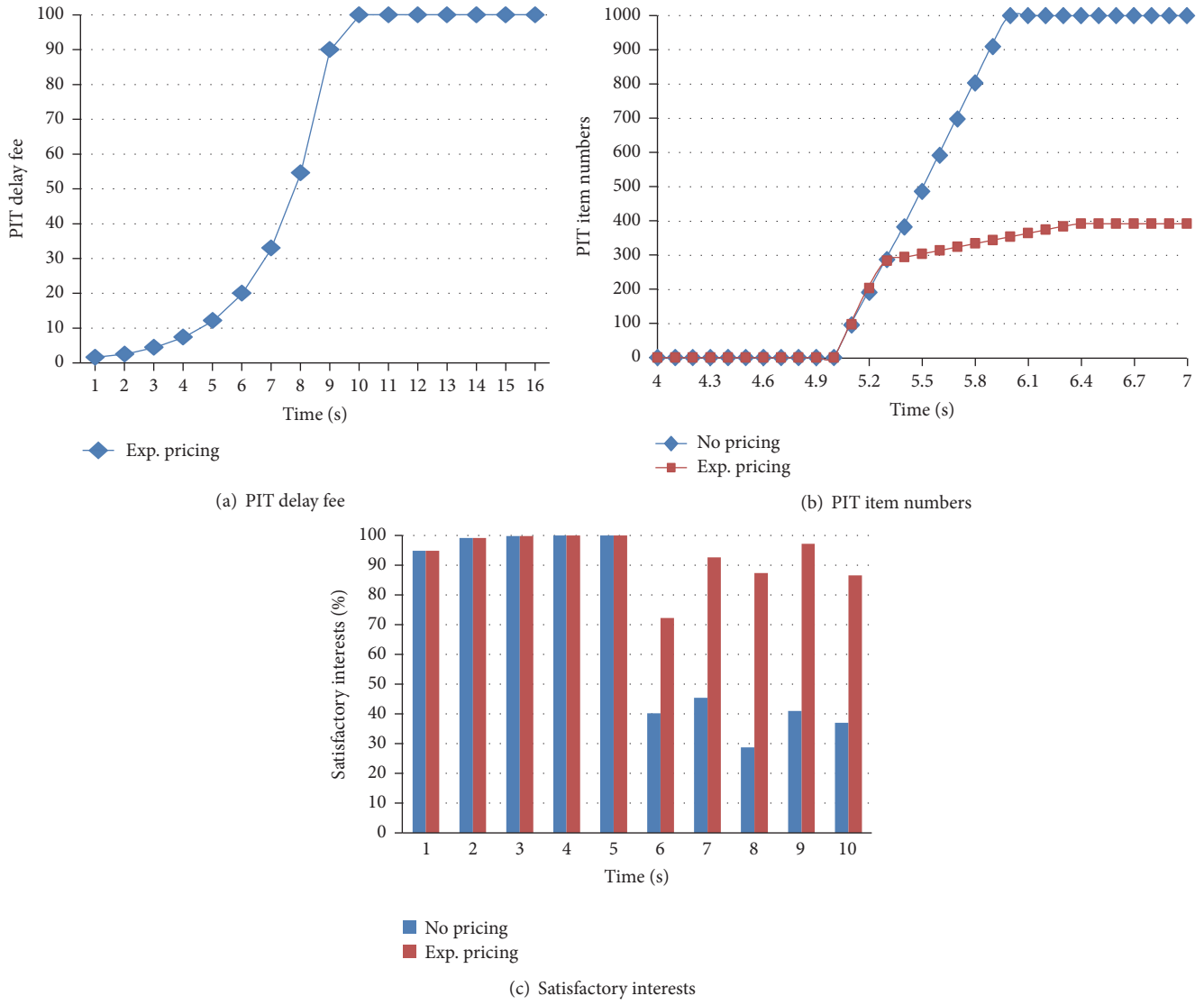
mechanism, downstreaming NDN nodes or end users are encouraged to submit/forward interest requests to those upstreaming nodes with more empty PIT entries. This is reasonable just like queue systems with multiple service windows in economic life.

(4) *Exponential Pricing Function.* The preserved PIT delay fee will be consumed according to exponential pricing function. This kind of charging can be viewed as *incremental* charging PIT delay fee and it will be an exponential function of delayed time in PIT table. This is rational since PIT entries are critical resource and thus cannot be occupied for long time by some "dead entries" (here, "dead entries" indicate those interest requests that cannot find matched contents).

To charge content delivering fee (i.e., cdf) in NDN, as well as in today's Internet, is a subtle problem. We know that bandwidth is also a critical resource. It seems that we should use exponential pricing function. However, this will encourage end users to split a single large request (say, "please download the whole book for me") into several small requests (say, "please download the ith chapter of the book for me") if they do not mind the delay of contents of the later chapters. This is unexpected since it runs in the opposite direction with respect to the "best effort" mechanism that is widely accepted in today's Internet and will continue to be useful in future Internet architectures, including NDN. Therefore, we suggest using asymptotic pricing function for charging content delivering fee. Partial reason for doing this is that within the same time-window and with the same local topology of network bandwidth has fixed limitation and from the view of NDN router node, local available bandwidth might be less critical than PIT entries.

In summary, the utilization of different pricing functions in NDN can be tabulated in Table 2.

3.4. Paying or Charging Content Producers? Seemingly, it is also reasonable to pay content producers, just like in economic life. However, since NDN architecture tries to play



(a) PIT delay fee

(b) PIT item numbers

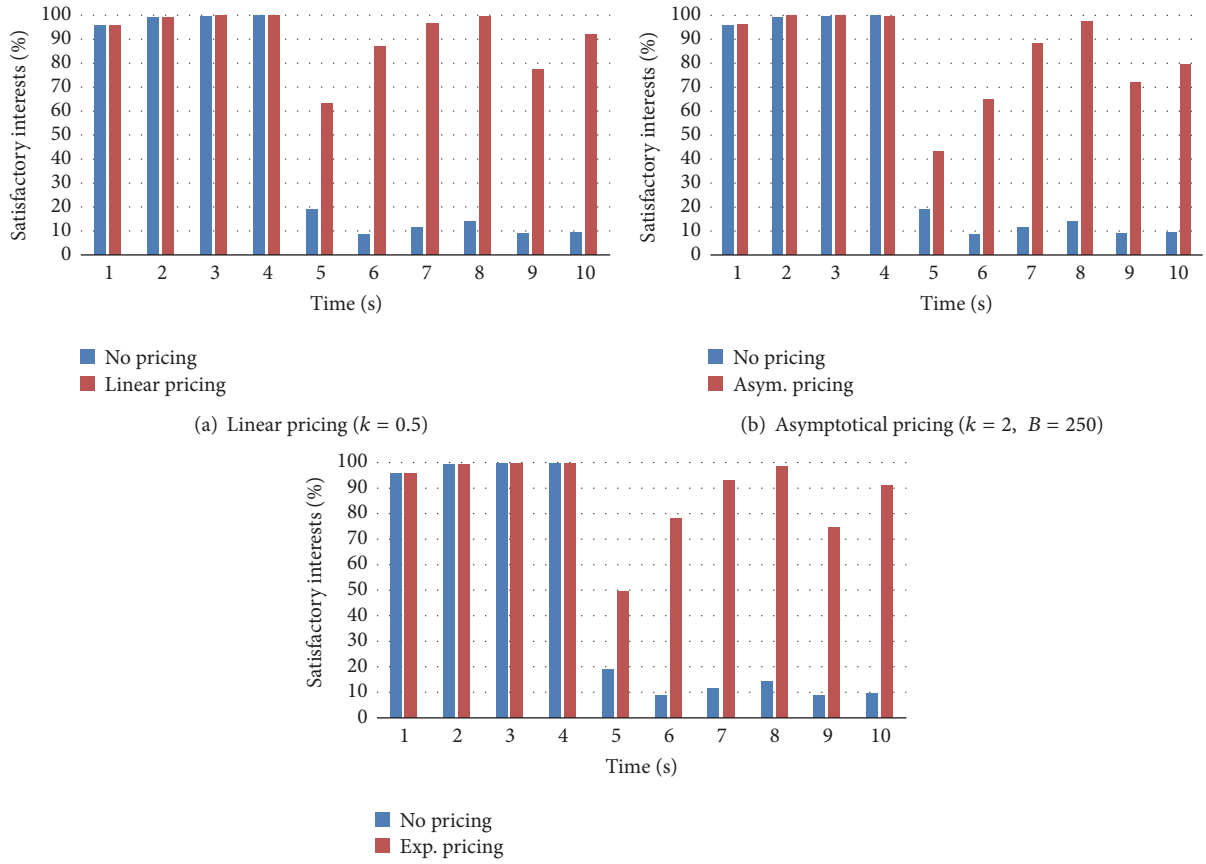
(c) Satisfactory interests

Figure 8: Simulation on exponential pricing strategy ($\alpha = 1$, $\beta = 0.02$).

Table 2: Utilization of pricing functions in NDN.

Pricing functions	Utilities/properties
Linear	Charging local interest request and PIT delay fee will increase linearly.
Asymptotic	PIT delay fee will become huge when PIT table reaches its limitations.
Exponential	The incremental PIT delay fee will increase exponentially.

down the concept of addressing and considering that many content packets will be cached in networking, the content producers cannot always fetch the real end users, and some NDN router node might be the last hop for forwarding interest request to content producers. Thus, the end users and the NDN routers have no sufficient prior knowledge to make proper prepayments to content producers. In fact, according to our abstraction of the proposed prototype, NDN router nodes need not consider the semantics of contents. Instead, NDN nodes just provide services of interests looking up and content delivering. In other words, NDN nodes play merely the role of logistics distribution, instead of the role of purchasing agents. Therefore, we suggest not to pay content producers. Moreover, in order to encourage NDN router nodes to perform better content delivering service, we can even ask content producers to pay NDN router nodes, and in return content producers can obtain what they deserved directly from the end users based on (post)accounting and auditing mechanisms. By doing so, another problem arises: How to protect content producers' benefits if a NDN router node sends many copies of some popular contents to many end users? Fortunately, this problem is essentially the issue of digital rights management (DRM) that has been studies extensively and there are a lot of mature solutions [26]. In other words, even if a NDN router node distributes many



(a) Linear pricing ($k = 0.5$)

(b) Asymptotical pricing ($k = 2$, $B = 250$)

(c) Exponential pricing ($\alpha = 1$, $\beta = 0.03$)

Figure 9: Simulation on a net-like topology.

copies of certain content, it merely gets multiple of content delivering fees, instead of the fee regarding the semantics and the quality of the content. If it charges more, it will face the risk of being detected and then have to afford punitive overcharging according to DRM or (post)auditing mechanisms.

4. Simulations and Evaluations

To verify the effectiveness of the proposed method, we conduct related simulations by using ndnSIM [16]. Our simulation is run over a PC workstation with 2.93 GHz CPU and 2 GB memory. The operation system is Windows 7, but the configurations and newly added specifications/functionalities of nsnSIM are implemented in Ubuntu that is running over a virtual machine created by VMware Workstation.

Our simulations are organized according to two different network topologies. The first is a very simple and tree-like topology that is merely used to illustrate our basic idea (see Figure 5(a)), while the second is a net-like topology that is randomly generated (see Figure 5(b)). For the first topology, there are in total 5 attack nodes (see grey nodes in Figure 5(a)) and they launch attack 5 seconds after the beginning of the corresponding simulations. For the second topology, we assume that all nodes behave normally at the beginning of the simulations, while after 4 seconds, 25 among them (i.e., about 15%) are randomly selected and specified as malicious. In both topologies, we, respectively, use linear pricing function, asymptotical pricing function, and exponential pricing function in charging PIT delay fee. In our simulations, the prepayment of an interest request is set to 100, and the maximum number of PIT items is set to 1000. Then, we collect related data and observe the evolution of not only the pricing function values, but also the numbers of unsatisfied interest requests in the related PIT tables (i.e., PIT item numbers) and the degree of satisfactory interest requests that is evaluated simply by the ratio of $n_s/(n_s + n_u)$, where n_s (resp., n_u) is the number of satisfied (resp., unsatisfied) interest requests.

Results are depicted in Figures 6, 7, 8, and 9, respectively.

(1) From Figures 6(a), 7(a), and 8(a), we can see different tendencies with different pricing functions. Note that in these pricing functions we always associate c in the related pricing functions with the number of interest requests coming from some ports, but based on our repeat testing we find that the results are a bit sensitive to other parameters like k, B, α, β, and so forth. In our simulations, we set these parameters based on the experience obtained from our earlier tests.

(2) From Figures 6(b), 7(b), and 8(b), we learn that on one hand, compared to the strategy without charging, these pricing functions are *indeed effective for keeping PIT tables from being quickly used out*; on the other hand, compared among these pricing functions, *the utility ratio of PIT tables with asymptotical pricing strategy is highest*, while the utility ratio of PIT tables with exponential pricing strategy is lowest.

(3) From Figures 6(c), 7(c), and 8(c), we learn that, compared to the strategy without charging, these pricing functions are *indeed effective for keeping high satisfactory ratio for newly coming interest requests on a long view*. But, this time, asymptotical pricing strategy does not manifest remarkable advantages over linear pricing strategy and exponential pricing strategy. In fact, the utility ratio of PIT tables and the satisfactory ratio for newly coming interest requests are interactions. To keep higher utility ratio of PIT tables means setting aside less room for newly coming interest requests and thus leading to lower satisfactory ratio. Therefore, we have to choose a balance between them. With this in mind, we think, as for the first simple topology, asymptotical pricing strategy outperforms the other two.

(4) However, from Figure 9, we can see that, as for the second topology, which is even close to real situations, asymptotical pricing strategy will lead to lowest satisfactory ratio for newly coming interest requests on a long view. Interestingly, linear pricing function outperforms the other two in this case. Again the proverb seems to be validated: *the simpler, the better.*

5. Summary and Future Work

An initial analysis of possibility of using economic levers in fighting interest flooding attacks (IFA) in Named Data Networking (NDN) is presented. We started by presenting a prototype for NDN that consists of seven basic business logics/steps, followed by an examination of compatibilities of existing micropayment systems and an analysis of utilization of some well-known pricing functions in NDN. Then, some basic simulations based on ndnSIM are developed and the results show that it is indeed effective for fighting IFA. Clearly, this is only the first step towards fighting DoS/DDoS in NDN with economic levers. More work is required to evaluate the effectiveness of the proposed prototype and to locate possible mismatched aspects of detailed business logics, such as the sensitiveness of different pricing functions with different setting on related parameters. Moreover, testbed-based, instead of simulation-based, experiments are needed for determining the real impacts of different micropayments and pricing functions on IFA in NDN.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Key Research and Development Program (no. 2016YFB0800602), the National Natural Science Foundation of China (NSFC) (nos. 61370194, 61502048), and the Engineering Planning Project of Communication University of China (no. 3132017XNG1720). The third author is also partially supported by JSPS KAKENHI Grant no. JP16K00117, KDDI Foundation.

References

[1] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "DoS and DDoS in named data networking," in *Proceedings of the 2013 IEEE 2013 22nd International Conference on Computer Communication and Networks, ICCCN 2013*, bhs, August 2013.

[2] W. Adjie-Winoto, E. Schwartz, H. Balakrishnan, and J. Lilley, "The design and implementation of an intentional naming system," *ACM SIGOPS Operating Systems Review*, vol. 33, no. 5, pp. 186–201, 1999.

[3] N. Tolia, M. Kaminsky, and D. Andersen, "An architecture for Internet data transfer," in *Proceedings of the 3rd conference on Networked Systems Design Implementation (NSDI*, pp. 253–266, 2006.

[4] T. Koponen, M. Chawla, B.-G. Chun et al., "A data-oriented (and beyond) network architecture," in *Proceedings of the ACM SIGCOMM 2007: Conference on Computer Communications*, pp. 181–192, jpn, August 2007.

[5] M. Caesar, T. Condie, J. Kannan, K. Lakshminarayanan, I. Stoica, and S. Shenker, "ROFL: routing on flat labels," in *Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications*, pp. 363–374, 2006.

[6] I. Stoica, D. Adkins, S. Zhuang, S. Shenker, and S. Surana, "Internet indirection infrastructure," *IEEE/ACM Transactions on Networking*, vol. 12, no. 2, pp. 205–218, 2004.

[7] Project PSIRP. http://www.psirp.org, 2010.

[8] V. Jacobson, "Special plenary invited short course: (CCN) Content-centric networking," in *Future Internet Summer School*, Germany, Bremen, 2009.

[9] Project CCNx. http://www.ccnx.org, 2011.

[10] V. Jacobson, D. Smetters K, J. Thorton D et al., "Networking named content," *Communications of the ACM*, vol. 55, no. 1, pp. 117–124, 2012.

[11] A. Juels and J. Brainard, "Client puzzles: a cryptographic defense against connection depletion attacks," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, pp. 151–165, 1999.

[12] V. Jacobson, D. K. Smetters, N. H. Briggs et al., "VoCCN: Voice-over content-centric networks," in *Proceedings of the 2009 workshop on Re-architecting the internet*, pp. 1–6, 2009.

[13] L. Zhang and D. Estrin, "Named data networking (NDN," Tech. Rep., 2010.

[14] Z. Zhu, S. Wang, X. Yang, V. Jacobson, and L. Zhang, "ACT: audio conference tool over named data networking," in *Proceedings of the 2011 ACM SIGCOMM Workshop on Information-Centric Networking, ICN 2011, Co-located with SIGCOMM 2011*, pp. 68–73, 2011.

[15] H. Yuan and P. Crowley, "Experimental evaluation of content distribution with NDN and HTTP," in *Proceedings of the IEEE INFOCOM 2013 Mini-Conference*, pp. 240–244, 2013.

[16] A. Afanasyev, I. Moiseenko, and L. Zhang, "ndnSIM, NDN simulator for NS-3," Tech. Rep., 2012.

[17] A. Atanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, "Interest flooding attack and countermeasures in named data networking," in *Proceedings of the IFIP Networking*, pp. 1–9, 2013.

[18] D. Mankins, R. Krishnan, C. Boyd, J. Zao, and M. Frentz, "Mitigating distributed denial of service attacks with dynamic resource pricing," in *Proceedings of the 17th Annual Computer Security Applications Conference, ACSAC 2001*, pp. 411–421, usa, December 2001.

[19] M. Abadi, M. Burrows, M. Manasse, and T. Wobber, "Moderately hard, memory-bound functions," in *Proceedings of the 10th Annual Network and Distributed System Security Symposium (NDSS)*, pp. 25–39, Internet Society, 2003.

[20] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in *Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO)*, pp. 139–147, Springer-Verlag, London, UK, 1992.

[21] Y. Shen, F. Fan, W. Xie, and L. Mo, "Re-Traffic pricing for fighting against DDoS," in *Proceedings of the 2008 ISECS International Colloquium on Computing, Communication, Control, and Management (CCCM)*, pp. 332–336, IEEE Computer Society, Washington, DC, USA, 2008.

[22] R. Rivest and A. Shamir, "PayWord and MicroMint: Two Simple Micro-payment Schemes, Proceeding of the Security Protocols Workshop," *Lecture Notes in Computer Science*, vol. 1189, pp. 69–87, 1997.

[23] S. C. Glassman, M. S. Manasse, M. Abadi, P. Gauthier, and P. Sobalvarro, "The Millicent protocol for inexpensive electronic commerce," *World Wide Web*, vol. 1, no. 1, 1996, https://www.w3.org/Conferences/WWW4/Papers/246/.

[24] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System. http://bitcoin.org.

[25] S. Khanna, S. S. Venkatesh, O. Fatemieh, F. Khan, and C. A. Gunter, "Adaptive selective verification: An efficient adaptive countermeasure to thwart DoS attacks," *IEEE/ACM Transactions on Networking*, vol. 20, no. 3, pp. 715–728, 2012.

[26] Q. Liu, R. Safavi-Naini, and N. P. Sheppard, "Digital rights management for content distribution," in *Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003 (ACSW Frontiers 2003)*, vol. 21, pp. 49–58, Australian Computer Society, 2003.