Analyzing NDN NACK on Interest Flooding Attack via SIS Epidemic Model

Kai Wang, *Member, IEEE*, Dongchao Guo, and Wei Quan, *Member, IEEE*

***Abstract*—Security properties are within the fundamental concerns in the original protocol stack of named data networking (NDN) paradigm. However, NDN still cannot evade some serious network attacks, such as the notorious interest flooding attack (IFA). To mitigate the IFA, interest Negative ACKnowledgments (NACK) may be one of the best countering candidates in NDN, yet does not attract enough concerns. In this paper, we first present a more powerful type of IFA using interest packets with real names rather than spoofed ones to confuse detections. Then, we evaluate the effectiveness of interest NACK on mitigating IFA via a modified susceptible-infected-susceptible epidemic model. In this quantitative analysis tool, we introduce a variable curing parameter to accurately characterize the impact of interest NACK on chosen NDN routers. Moreover, we derive the upper bound for the infection fraction of NDN routers with and without interest NACK, and deduce the relationship between the fraction of total infected nodes and those with NACK implementation. In addition, the accuracy of the proposed model is verified by extensive simulations. To the best of our knowledge, this is the first attempt to theoretically analyze the NDN NACK mechanism on mitigating IFA via the epidemic theory.**

***Index Terms*—Epidemic model, future Internet, interest Negative ACKnowledgments (NACK), interest flooding attack (IFA), named data networking (NDN).**

I. Introduction

NAMED data networking (NDN) [1], which inherits the core design ideas from an earlier project named content-centric networking (CCN) [2], is a promising architecture for future Internet, due to its higher efficiency and better security than traditional IP-based networking paradigm. NDN has great potential for supporting future mobile Internet [3], [4], vehicle networks [5], [6], and software-defined network (SDN) [7], [8], making it a very popular topic in future Internet researching areas. From the security perspective, NDN decouples the security of content from the single point-to-point conversation to self-authenticating data itself. In this way, NDN reduces the trust in network intermediaries, opening the network as well as providing more convenience to wide participation [9].

Comparing to the traditional five layers, which are application layer, transport layer, network layer, link layer, and physical layer in TCP/IP networking paradigm, NDN introduces two new layers, which are the security layer and strategy layer, into its original protocol stack [1]. The strategy layer is to achieve efficient packet forwarding and retrieving by taking maximum advantage of multiple connectivities simultaneously (e.g., retrieving different data pieces of the same content from multiple network interfaces with different types such as ethernet, fiber, bluetooth and 5G) [10], [11]. That is, NDN supports multicast communications natively. On the other hand, the security layer enables NDN to secure data directly and built trust in data itself [12]. Specifically, the security of NDN is guaranteed by securing data instead of communication channels over which a packet travels, thus the trust is directly built on the security properties of data (e.g., digital signatures) rather than where and how they are obtained [13]. Secure channel access (e.g., IPSec or TLS secure channels) is popular in TCP/IP networking, but cannot directly translate to data security, as data could be altered before sent into this channel. Moreover, each IP data packet may lose cryptographic protection when leaving its transmitted channel, yet every NDN data packet is self-identifying, self-authenticating, and idempotent. Consequently, each data piece of any content in NDN is potentially valuable and useful to a large amount of consumers, since one can publicly validate the retrieved content with its own digital signature no matter where it is retrieved, enabling ubiquitous content caching in everywhere of the network to improve content transmission efficiency [14]. As a comparison, securing channels between every pair of the communication endpoints can quickly cause scalability and manageability problems, when there are multiple parties need to communicate at the same time.

Although security is among the key concerns in the very early design of NDN protocol stack, it still cannot evade the damage from network threats. Particularly, interest flooding attack (IFA) may be the most notorious malicious activity in NDN scenario [9], [15]. IFA exploits the NDN's inherit weaknesses that all the communication states for every forwarded interest packet should be cached in the pending interest table (PIT) of each involved router. Specifically, IFA can easily exhaust the memory resource of key routers by sending numerous malicious interest packets (e.g., interests with spoofed content names to avoid content hit in routers) to occupy the PIT. As a result, legitimate interest packets are very likely to be dropped by a router due to its PIT exhaustion.

Manuscript received December 27, 2018; revised April 17, 2019; accepted June 2, 2019. Date of publication July 22, 2019; date of current version June 3, 2020. This work was supported in part by the National Natural Science Foundation of China under Grant 61702439 and in part by the Shandong Provincial Natural Science Foundation, China under Grant ZR2017BF018. *(Corresponding author: Dongchao Guo.)*

K. Wang is with the School of Computer Science and Technology, Harbin Institute of Technology, Weihai 264209, China (e-mail: dr.wangkai@ieee.org).

D. Guo is with the School of Computer Science, Beijing Information Science and Technology University, Beijing 100101, China (e-mail: dongchaoguo@gmail.com).

W. Quan is with the Beijing Jiaotong University, Beijing 100044, China (e-mail: weiquan@bjtu.edu.cn).

Digital Object Identifier 10.1109/JSYST.2019.2923841

Unfortunately, except for the existence of the requested content, there are no other critical differences between legitimate and malicious interest packets [16], [17], making the accurate IFA premitigation on involved routers unpractical.

In addition, the component *MustBeFresh* (see NDN Packet Format Specification 0.3: http://named-data.net/doc/NDN-packet-spec/current) in each NDN interest packet even opens a new way for IFA to harm NDN by using real interest names, which is neglected by other research works. This paper addresses the aforementioned gap in the literature. If the *MustBeFresh* component is enabled in an interest, it indicates that the content store of intermediate routers cannot be used to respond this interest with its stale data, and thus this interest can be finally forwarded to the content server where fresh data is originally produced. Unfortunately, attackers can take advantage of this component to launch a new type of IFA by using interest packets with real names instead of fake ones, but it can still evade content hit at intermediate routers meanwhile maliciously occupy the PIT like the traditional IFA. As the attacking traffic from this type of IFA uses real names to masquerade as legitimate interest packets, detection of this attack becomes more difficult.

Considering IFA may lead to a wide crash of NDN forwarding plane, many efforts are made to defend against this type of attack [9]. However, most of the pervious works mainly focus on how to detect and mitigate IFA, but neglect to give a fundamentally mathematical model that can accurately characterize its inherit features [18], which makes the countermeasure designs inefficient or even totally impractical. Designing such a theoretical model will give an illuminating insight for the IFA research, and provide great help to the design of more effective and adaptive countermeasures. From the perspective of network science, IFA can be treated as an information diffusion process [18], and one of the best theoretical frameworks that can characterize the dynamics of many information diffusion processes (e.g., viruses, rumors or malicious flows) is the epidemic diffusion model [19].

In this paper, we first employ the in-homogeneous susceptible-infected-susceptible (SIS) process, which is one typical type of epidemic diffusion models, to model the flow of malicious traffic from IFA in NDN. Then, we modify the N-intertwined mean-field approximation model (NIMFA) [20], [21] and named it as heterogeneous NIMFA model (HNIMFA), to analyze the dynamics of the epidemic process with in-homogeneous infection rate and recovering rate, and to evaluate the damage effect of IFA as well as find some key insights into the network security of NDN.

The main contributions of this paper are as follows.

1) A new type of IFA using interest packets with real names, rather than spoofed names, is introduced, which may be neglected by other works. Specifically, the *MustBeFresh* component in each NDN interest packet is enabled in this IFA, and thus all malicious interests can be routed to the content server at the edge, without satisfied by content store in any intermediate routers along the way. As a result, all the involved routers are attacked because their PITs are maliciously occupied by these interests. This new type of IFA provides a way for attackers to carry out a wide range of network attacks more covertly, by simply exploiting the vulnerabilities of the original NDN protocols.
2) A comprehensive taxonomy for the IFA research is given, where the efforts are divided into five types: IFA variants or advanced IFA, IFA modeling, IFA detecting and mitigating, stateless NDN, and the interest Negative ACKnowledgments (NACK). This taxonomy provides a quick and clear guide for relevant IFA researchers to conduct more professional researches in various subdivided fields.
3) A mathematical model for analyzing IFA, named HNIMFA, is given. HNIMFA can characterize the effect of interest NACK on defending IFA in a finite-size network. The accuracy of the proposed HNIMFA is demonstrated by simulation experiments. According to the results from both theoretical model and simulation experiments, the urgency of implementing interest NACK into as many as NDN routers is apparent and highlighted.

The rest of this paper is organized as follows. Section II introduces the background of SIS epidemic models and interest NACK. Section III gives a comprehensive taxonomy of the efforts on IFA studies. Section IV presents the details of the proposed IFA analyzing model (HNIMFA) with theoretical results. Section V investigates and evaluates the accuracy of the proposed theoretical model via simulations. Finally, Section VI concludes this paper.

II. Background

In this section, we present some closely related background to our work. We first give a brief introduction on SIS epidemic models, and then explain why we select interest NACK as our analyzing target in the proposed HNIMFA model.

A. SIS Epidemic Model

Pastor–Satorras and Vespignani [22] proposed the heterogeneous mean-field approximation (HMFA) to model the epidemic process in an infinite network with nonhomogeneous degree distributions, and succeeded in deriving the epidemic threshold and the steady-state infection fraction. On the other hand, for a finite network, it is of interest to investigate the metastable state of the epidemic process since the only final stable state is the healthy state where all nodes are healthy [20]. Resorting to the mean-field approximation and the spectral graph theory, Van Mieghem *et al.* [20], [23] proposed the N-intertwined mean-field approximation (NIMFA) as the theoretical framework to investigate the continuous-time epidemic process with constant infection rate β and curing rate δ. Van Mieghem *et al.* derived the expression for the metastable-state infection fraction and revealed that the epidemic threshold $\tau_c = \beta/\delta$ is upper-bounded by the largest eigenvalue $\lambda_{\max}(A)$ of the adjacency matrix of the underlying topology. In another report [21], Van Mieghem *et al.* generalized the NIMFA model to the configuration with nonconstant and in-homogeneous infection rate β_i and curing rate δ_i for each individual node i. The generalized NIMFA can model the diffusion of user requests as epidemic spreading process through the whole network, which can help to characterize IFA on NDN.

B. Interest NACK

We only select interest NACK into our model due to its super importance to NDN. For instance, among all the current IFA countermeasures, interest NACK is the only one that has already been patched into the original NDN protocol stack, in both its real-world deployment–NDN forwarding daemon (NFD) [24] and its official simulation platform–ndnSIM [25], [26]. Other IFA countermeasures may be also effective, yet have not been embedded into either the NDN official implementation or any version of its simulation platform, thus they are not considered in our analyzing model. Interested readers for the state-of-the-art IFA countermeasures (including NACK) as well as their comparison can move on to these two comprehensive surveys [9], [27]. Interest NACK can indicate routers about the forwarding failures (e.g., forwarding to the place where data are not exist) with NACK message sent by content servers, which can flush the PIT entries and enable attacked routers to recovery at a much smaller time scale rather than waiting for entries timeout. Moreover, the latest emerging low-latency message forwarding technology can ensure the NACK messages to be transported reliably even in resource-constrained environments [28]. However, currently, interest NACK has not been widely accepted by NDN communities, and even some researchers suggest to avoid interest NACK in NDN. For instance, the CCNx team has announced that interest NACK is no longer implemented at the network layer in the latest release CCNx, instead treats it as a higher-layer functionality implemented as requirements [29]. In this paper, we argue the significant effect of interest NACK on mitigating IFA, and recommend to embed it into NDN's network layer directly for better security, based on our model results.

III. Taxonomy for IFA Research

The existence of IFA is first predicted when CCN, which is the predecessor of NDN, is proposed [30]. Then the work in [15] gives a detailed view on this type of NDN-specific network attack, including the launching principle of IFA (e.g., targeting a specific namespace), analysis of its damage on the network functionality, and its mitigation methods (e.g., satisfaction-based pushback). Inspired by the above efforts on defending IFA, many solutions have been proposed since then (see the survey [9] for more details).

To clearly describe different directions on this area, we suggest that the IFA studies can be divided into five types: IFA variants or advanced IFA, IFA modeling, IFA detecting and mitigating, stateless NDN, and interest NACK.

1) *IFA variants or advanced IFA:* Except for the original type of IFA, some advanced versions are introduced, showing the variants can bring in much more damage on NDN, such as the bIFA [31] that can generate malicious interests for both existent and nonexistent content, the AIFA [32] that can exhaust the PIT of a router without causing expired entries, and the CIFA [33] where malicious clients and servers launch an attack cooperatively. All these IFA variants enhance the destructiveness compared to their original version, and increase the difficulty of detection and mitigation.
2) *IFA modeling:* Modeling the impact of IFA via mathematical theories. For example, the works in [34] and [35] characterize the IFA damage by treating NDN PIT as a queueing system (e.g., M/G/c/c model [36]) with limited service time, and finally deduce an analytical model, to gain a better understanding on what type of circumstances makes PIT more or less vulnerable. Different from those works, the epidemic model is first introduced into NDN by the effort in [18], and then used to model the damage effect of IFA by treating each NDN router as infected or cursed depending on whether there is any spoofed Interest recorded in its PIT or not. All these efforts on modeling IFA give insight for the inherent features of this attack, and can guide better designs for the IFA countermeasures.
3) *IFA detecting and mitigating:* Methods on directly detecting and mitigating IFA. The former focuses on how to identify the existence of IFA, while the latter aims at limiting the damage caused by IFA. Specifically, IFA detecting methods are mainly based on investigating the dynamic features of interests under certain prefixes (e.g., cumulative entropy of abnormal interests distribution [37], the Gini impurity for each data prefix [38], the power spectral density of all the incoming interests [39], interest satisfaction ratio [15], [40]–[42], number of expired PIT entries [43], combination of expired PIT entries and PIT size [44], combination of interest satisfaction ratio and PIT size at each interface within a router [45], interest existence judged by content server [46], [47]), while IFA mitigating methods are mainly rate-limit mechanisms (e.g., filtering traffic based on data prefixes [38], [42], [43] or router interfaces [15] or certain security tokens cached in routers [46]).
4) *Stateless NDN:* Redesigning the architecture of NDN by decoupling interest states from PIT. Different from the efforts on how to limit the consumption of PIT, the authors in [16] argue the stateful forwarding plane open a gate for router memory exhaustion attacks (e.g., IFA), and it may not be a mandatory NDN feature. They design a stateless NDN architecture without PIT instead, in which data packets are routed via backwards routable names rather than PIT pending states. Similarly, the work in [48] also abandons PIT, and instead embeds a route token into the name component of each interest packet, which then enables every router to successfully find the incoming interface for every requested data packet. Different from them, in our previous work, termed as DPE [17], only malicious interests are decoupled from PIT to decrease router's resource exhaustion, but legitimate interests are still cached in PIT to achieve stateful data forwarding. The consensus of all these solutions is the stateless forwarding plane for malicious interests.
5) *Interest NACK:* Updating NDN by embedding interest NACK into its protocol stack. Comparing to the clean-slate solutions, such as the stateless NDN, interest NACK [29] may be a more practical mechanism to effectively defend IFA meanwhile maintain the original stateful forwarding plane for NDN. As evaluated in our previous work

TABLE I
NOTATIONS AND MEANINGS

Symbol	Meaning
$G(\mathcal{N}, \mathcal{L})$	A graph G with $\lvert\mathcal{N}\rvert = N$ nodes and $\mathcal{L} = L$ links.
$A := \{a_{ij} \lvert 0, 1\}$	The adjacency matrix of a graph with elements a_{ij}
$\lambda_{\max}(A)$	The largest eigenvalue of the matrix A.
$u^T = \{1, \ldots, 1\}$	The all one vector.
$d_i = \sum_{j=1}^{N} a_{ij}$	The degree of node i.
$d_{\min} = \min_j d_j$	The minimum degree.
$X_i(t) \in \{0, 1\}$	The viral state of node i at time t.
$v_i(t) = \Pr[X_i(t) = 1]$	The probability that the node i is in the infected state at time t.
β_i	The rate of the infection process per link which is a Poisson process.
δ_i	The rate of the curing process which is a Poisson process.
$\tau_i = \beta_i/\delta_i$	The effective infection rate of the node i.
$v_{i\infty} = \lim_{t\to\infty} v_i(t)$	The steady-state infection probability of the node i.
$y_\infty = \sum_{i=1}^{N} v_{i\infty}/N$	The steady-state infection fraction, i.e., the number of infected nodes when $t \to \infty$.
$v_{\min\infty} = \min_j v_{j\infty}$	The minimum value of the steady-state infection probability among all nodes.

[32], NACK mechanisms can significantly degrade the damage of IFA, as the malicious pending interests can be removed immediately from routers when NACK packets arrive, rather than caching them until PIT timeout. As a result, the average duration of each malicious interest in PIT is decreased from the level of time-to-live (TTL) in seconds [11] to round trip time (RTT) in milliseconds [49], [50]. In addition, the interest traceback [51] is also one kind of NACK mechanisms, and it can traceback the attacking originator by spoofing corresponding data packet to respond each malicious interest along its attacking path.

IV. THEORETICAL MODEL FOR IFA

We start by rehearsing the HNIMFA model. Then, we present some theoretical results for the steady-state infection fraction, the time evolution of the epidemic process, the epidemic threshold, and some trivial cases.

A. Model Definition

Notations used in the model are summarized in Table I. We consider two independent Poisson processes in an undirected unweighted graph $G(N, L)$, which is composed of N nodes and L links, namely the infection process and the curing process. The concerned finite-size network is denoted by an adjacency matrix A with elements a_{ij}. The viral state $X_i(t)$ of the node i of the network at time t is represented by a Bernoulli random variable defined as $X_i(t) \in \{0, 1\}$: $X_i(t) = 0$ for the *healthy* but *susceptible* state, or $X_i(t) = 1$ for the *infected* state. In other words, the node i could be either in the infected state with probability $v_i(t) = \Pr[X_i(t) = 1]$ or in the healthy state with probability $1 - v_i(t) = 1 - \Pr[X_i(t) = 1]$. For a Bernoulli random variable, the relation $E[X_i] = \Pr[X_i = 1]$ holds. An infected node i will recover with rate δ_i. The infection process per link connecting an infected node i and a susceptible node j is a Poisson process with rate β_i. Only a node is infected, it could infect its neighbors which are in the healthy states. The aforementioned curing process and the infection process constitute the heterogeneous susceptible-infected-susceptible (SIS) epidemic process. For the configuration where $\beta_i = \beta$ and $\delta_i = \delta$ are constants, the heterogeneous SIS process reduces to the classic SIS process which we name as the homogeneous SIS process. The degree d_i of the node i is defined as $d_i = \sum_j a_{ij}$. Another critical notation is the effective infection rate defined as $\tau_i = \beta_i/\delta_i$.

To analyze the IFA, a NDN node is defined as *infected* if there is any malicious interest recorded in its PIT. Different from the mechanism in [18], in our model, the duration of some malicious interests may be evicted from router memory at a much quicker manner due to the responded NACK messages, rather than waiting for PIT timeout. A NDN node is considered as *susceptible* if no malicious interests are cached in its PIT, which means no expired PIT entry appears and meanwhile no NACK message indicating nonexist data is received within the monitoring window.

Based on the description above, there are two possible values for the curing rate δ for analyzing IFA in our proposed theoretical model. When a NDN node is implemented with the NACK mechanism, it will be cured to *susceptible* state at the time-scale of RTT level, and this cursing rate is termed as δ_a. However, if it is not enabled with NACK, it will be kept in *infected* state until the corresponding PIT entry expired, which is much longer than RTT (usually three orders of magnitude larger than RTT [11], [49]), and this cursing rate is termed as δ_b ($\delta_b > \delta_a$).

To simplify the analyzing model, we configure every NDN router with the same forwarding strategy to achieve a constant β, and thus can strictly focus on how the fraction of NACK-enabled NDN nodes affects the impact of IFA.

The heterogeneous SIS process, consisting of the aforementioned two Poisson processes, i.e., the infection process and the curing process, can be formulated exactly by the following ordinary differential equation:

$$\frac{d}{dt}E[X_i(t)] = E\left[-\delta_i X_i(t) + (1 - X_i(t))\sum_{j=1}^{N}\beta_j a_{ji} X_j(t)\right]. \tag{1}$$

Applying the mean-field approximation methodology, the differential equation (1) could be simplified and rewritten as the

following form [20], [21]:

$$\begin{aligned}\frac{d}{dt}v_i(t) &= -\delta_i v_i + (1-v_i)\sum_{j=1}^{N}\beta_j a_{ij} v_j \\ &= \sum_{j=1}^{N}\beta_j a_{ji} v_j(t) - v_i(t)\left(\sum_{j=1}^{N}\beta_j a_{ji} v_j(t) + \delta_i\right)\end{aligned} \tag{2}$$

where the assumption $E[X_iX_j] = E[X_i]E[X_j]$ is used. According to the governing equation (2) of the infection probability of the node i, the time evolution of the viral state for each node could be expressed as

$$\begin{aligned}&\frac{d}{dt}v_1(t) = \sum_{j=1}^{N}\beta_j a_{j1} v_j(t) - v_1(t)\left(\sum_{j=1}^{N}\beta_j a_{j1} v_j(t) + \delta_1\right) \\ &\cdots \\ &\frac{d}{dt}v_N(t) = \sum_{j=1}^{N}\beta_j a_{jN} v_j(t) - v_N(t)\left(\sum_{j=1}^{N}\beta_j a_{jN} v_j(t) + \delta_N\right).\end{aligned} \tag{3}$$

With the following notations $V(t) = [v_1(t), v_2(t), \ldots, v_N(t)]^T$, $C = [\delta_1, \delta_2, \ldots, \delta_N]^T$, and $\mathrm{diag}(v_i(t))\, C = \mathrm{diag}(\delta_k)\, V(t)$, we arrive at

$$\begin{aligned}&\frac{d}{dt}V(t) \\ &= A\mathrm{diag}(\beta_j)V(t) - \mathrm{diag}(v_i(t))\left(A\mathrm{diag}(\beta_j)V(t) + C\right) \\ &= \left(A\mathrm{diag}(\beta_j) - \mathrm{diag}(v_i(t))A\mathrm{diag}(\beta_j) - \mathrm{diag}(\delta_k)\right)V(t) \\ &= \left(\mathrm{diag}(1-v_i(t))A\mathrm{diag}(\beta_j) - \mathrm{diag}(\delta_k)\right)V(t)\end{aligned} \tag{4}$$

which represents the governing equations (3) in the matrix form.

In the following, we confine ourselves to the configuration where $\beta_i = \beta$ for each node i. Although this case is more general than what we are concerned within this paper, it is intriguing to get more theoretical results under this general framework.

B. Steady-State Infection Probability and Infection Fraction

The steady state, denoted by $v_{i\infty}$, implies $\frac{dv_i(t)}{dt}_{t\to\infty} = 0$, and thus we could rewrite the infection probability (2) for each node i as

$$\delta_i v_{i\infty} = (1 - v_{i\infty})\sum_{j=1}^{N}\beta_j a_{ij} v_{j\infty}. \tag{5}$$

Rewritten in an iterative form, yields

$$\begin{aligned}v_{i\infty} &= \frac{\sum_{j=1}^{N}\beta a_{ij} v_{j\infty}}{\sum_{j=1}^{N}\beta a_{ij} v_{j\infty} + \delta_i} \\ &= 1 - \frac{1}{1 + \tau_i \sum_{j=1}^{N} a_{ji} v_{j\infty}} \\ &= 1 - \frac{1}{1 + \tau_i d_i - \tau_i \sum_{j=1}^{N} a_{ij}\left(1 - v_{j\infty}\right)} \\ &= 1 - \frac{1}{1 + \tau_i d_i - \tau_i \sum_{j=1}^{N} a_{ji} \frac{1}{1+\tau_j \sum_{k=1}^{N} a_{kj} v_{k\infty}}} \\ &= 1 - \frac{1}{1 + \tau_i d_i - \tau_i \sum_{j=1}^{N} a_{ji} \frac{1}{1+\tau_j \sum_{k=1}^{N} a_{kj} \frac{1}{\ddots}}}.\end{aligned} \tag{6}$$

By the nonlinear expression (5), we could calculate, in general, the steady-state infection fraction, defined as

$$y_\infty = \lim_{t\to\infty}\frac{\sum_{i=1}^{N} v_i(t)}{N} = \frac{\sum_{i=1}^{N} v_{i\infty}}{N}. \tag{7}$$

With the above equation and the symmetry property $a_{ij} = a_{ji}$, we could get an upper bound of the steady-state infection probability $v_{i\infty}$

$$\begin{aligned}v_{i\infty} &= 1 - \frac{1}{1 + \tau_i d_i - \tau_i \sum_{j=1}^{N} a_{ji}(1 - v_{j\infty})} \\ &\le 1 - \frac{1}{1 + \tau_i d_i}\end{aligned} \tag{8}$$

where $\tau_i = \beta/\delta_i$ and $d_i = \sum_{j=1}^{N} a_{ij}$.

We define the minimum steady-state infection probability $v_{\min\infty}$ as $v_{\min\infty} = \min_j\{v_{j\infty}\}$ and the minimum nodal degree $d_{\min}$ as $d_{\min} = \min_j\{d_j\}$. One lower bound of the steady-state infection probability is

$$\begin{aligned}v_{i\infty} &= 1 - \frac{1}{1 + \tau_i \sum_{j=1}^{N} a_{ji} v_{j\infty}} \\ &\ge 1 - \frac{1}{1 + \tau_i \sum_{j=1}^{N} a_{ji} v_{\min\infty}} \\ &\ge 1 - \frac{1}{1 + \tau_i d_{\min} v_{\min\infty}}.\end{aligned} \tag{9}$$

Hence, we get the bounds of the infection probability $v_{i\infty}$, which are written as

$$1 - \frac{1}{1 + \tau_i d_{\min} v_{\min\infty}} \le v_{i\infty} \le 1 - \frac{1}{1 + \tau_i d_i}. \tag{10}$$

The governing equations (3) describe how the SIS process evolves in the networks composed of the NDN routers. Equation (5) specifies the probability of the router i being infected in the steady state. The physical meaning of (7) stands for the average fraction of routers being in the infected state when the system is in the steady state. Albeit involving some computational complexity, we could calculate, in general, the average number of routers being infected in the steady state, incorporating (7) and (5). At the cost of accuracy, (6) defined in an iterative way, could provide an approximate estimate of the steady-state infection probability $v_{i\infty}$. For those who are only concerned with bounds rather than accurate values of the steady-state infection fraction, the inequality (10) provides a more efficient way to get rough predictions.

C. Time Evolution

We focus on the case where $V(t)$ is enough small to ignore the term $\mathrm{diag}(v_i(t))A\mathrm{diag}(\beta_j)$ in (4). The time-dependent solution is

$$\frac{d}{dt}V(t) = (\beta A - \mathrm{diag}\,(\delta_k))\,V(t). \tag{11}$$

The solution of the above ordinary differential equation is

$$V(t) = e^{(\beta A - \mathrm{diag}(\delta_k))t}V(0). \tag{12}$$

Written in another form, with the definition $W = \beta A - \mathrm{diag}\,(\delta_k)$, leads to

$$V(t) = P^T \mathrm{diag}\left(e^{\tilde{\lambda_i}t}\right)PV(0) \tag{13}$$

where $W = P^T \mathrm{diag}\left(e^{\tilde{\lambda_i}}\right)P$ and $\tilde{\lambda_i}$ denotes the eigenvalue of the composite matrix W.

Equations (12) and (13) give insights into the time evolution of the SIS process. The merits of the time evolution governing equation are two folds. It first provides a practical method to roughly measure the properties of the SIS process as a function of time. Its form also implies that the viral state drops exponentially to the absorbing state as the time increases given that the infection rate is below the critical value.

D. Epidemic Threshold

It is of interest to introduce the theorem of the epidemic threshold of the heterogeneous SIS model. The epidemic threshold is the vector $(\tau_{1c}, \ldots, \tau_{Nc})$ obeying the relations $\lambda_{\max}(R) = 1$ where the eigenvalue $\lambda_{\max}(R)$ is the largest one of the matrix

$$R = \mathrm{diag}\,(\sqrt{\tau_i})\,A\mathrm{diag}\,(\sqrt{\tau_i})\,. \tag{14}$$

The study of the epidemic threshold reveals that the epidemic threshold of the homogeneous SIS process, which could be regarded as a trivial configuration of the heterogeneous SIS process, is upper bounded by the largest eigenvalue of the underlying topology [20]. However, we still know little about the steady-state infection fraction and the epidemic threshold of the nontrivial heterogeneous SIS process under the framework of the proposed HNIMFA (4).

The Rayleigh quotient gives the upper bound of the largest eigenvalue, i.e.,

$$\lambda_{\max}(R) = \sup_x \frac{x^T R x}{x^T x} \tag{15}$$

where x is any possible N-dimensional vector. Different choices of the vector x lead to various bounds on the largest eigenvalue.

At the critical threshold where $\lambda_{\max}(R) = 1$, the following bounds (see [21, Eq. 13])

$$\lambda_{\max}(A) \min_{1\le j\le N} \tau_j \le \lambda_{\max}(R) \le \lambda_{\max}(A) \max_{1\le j\le N} \tau_j \tag{16}$$

reduce to another form

$$\tau_{\min;c} \le \frac{1}{\lambda_{\max}(A)} \le \tau_{\max;c} \tag{17}$$

where notations $\tau_{\min;c} = \min_{1\le j\le N}\tau_j$ and $\tau_{\max;c} = \max_{1\le j\le N}\tau_j$. For our concerned NDN case where $\tau_{i;c} = \{\beta_c/\delta_a, \beta_c/\delta_b\}$, the bounds reduce to

$$\frac{\delta_b}{\lambda_{\max}(A)} \ge \beta_c \ge \frac{\delta_a}{\lambda_{\max}(A)}. \tag{18}$$

With the choice $x = u$ of the vector and $u^T = \{1, \ldots, 1\}$, the Rayleigh quotient (15) reduces to

$$\begin{aligned}\lambda_{\max}(R) &\ge \frac{2L}{\sum_{j=1}^{N}\tau_j^{-1}} \\ &= \frac{E[D]}{E[\tau^{-1}]}\end{aligned} \tag{19}$$

which is derived in [21]. For our concerned NDN case where $\tau_i = \{\beta/\delta_a, \beta/\delta_b\}$, the bound reduces to

$$\lambda_{\max}(R) \ge \frac{\beta E[D]}{p\delta_a + (1-p)\delta_b} \tag{20}$$

where p denotes the fraction of nodes equipped with NACK. Besides, this lower bound is strict enough for regular graphs with constant average degree.

With (14) and the definition of the epidemic threshold $\lambda_{\max}(R) = 1$, we could determine the components of the vector of the effective infection rate $\vec{\tau_c} = (\tau_{1c}, \ldots, \tau_{Nc})$. It is obvious that there are almost infinite combinations of the components at the critical threshold. The simplest case is the homogeneous SIS process where $\tau_c = 1/\lambda_{\max}(A)$ with $\beta_i = \beta$ and $\delta_i = \delta$ for each node i. Besides, the bounds (17) and (19) give methods to roughly evaluate the critical infection rate at the critical threshold. The intentional attackers may design better attack approaches based on the evaluated bounds (18) and (20).

E. Special Cases

In the following, we take as example the complete graph. Assuming $\delta_{i\infty} = \{\delta_a, \delta_b\}$ and $\delta_a \le \delta_b$, the following relation holds for the complete graph:

$$v_{i\infty}(\delta_a) \ge v_{j\infty}(\delta_b) \tag{21}$$

where $v_{i\infty}(\delta_i)$ is considered a function of δ_i. We denote $v_a = v_{i\infty}(\delta_a)$ and $v_b = v_{j\infty}(\delta_b)$. With $b = Np$ and $N = a + b$, one could derive the steady-state infection probability

$$\delta_a v_a = \beta\,(1 - v_a)\,((a-1)\,v_a + bv_b) \tag{22}$$

$$\delta_b v_b = \beta\,(1 - v_b)\,((b-1)\,v_b + av_a)\,. \tag{23}$$

After some manipulations, written in the quadratic form, yields

$$\beta(a-1)v_a^2 + (\delta_a - \beta\,(a-1) + \beta b v_b)\,v_a - \beta b v_b = 0 \tag{24}$$

$$\beta(b-1)v_b^2 + (\delta_b - \beta\,(b-1) + \beta a v_a)\,v_b - \beta a v_a = 0. \tag{25}$$

The steady-state infection fraction could thus be calculated

$$y_\infty = (1-p)v_a + pv_b. \tag{26}$$

Then, we consider the epidemic threshold. The zeros of $\det(R - \lambda I)$ satisfy the equation [(18)], [21]

$$\sum_{j=1}^{N} \frac{1}{\tau_j + \lambda} = \frac{N-1}{\lambda}. \tag{27}$$

At the critical threshold, with $\lambda_{\max}(R) = 1$, the vector components of the critical effective infection rate satisfy

$$\sum_{j=1}^{N} \frac{1}{\tau_j + 1} = \frac{N-1}{1}. \tag{28}$$

For the configuration of NDN NACK, with $\tau_{i;c} = \{\beta_c/\delta_a, \beta_c/\delta_b\}$, we obtain the following equation:

$$\frac{p}{\tau_{a;c}+1} + \frac{(1-p)}{\tau_{b;c}+1} = \frac{N-1}{N} \tag{29}$$

which could be used to calculate the critical infection rate β_c. If the infection rate is larger than β_c, there is always some nonzero percentage of nodes being infected in the steady state.

V. Model Evaluation

In this section, the accuracy of the proposed HNIMFA is verified by simulation experiments in not only a complete topology but also a realistic Internet topology (the AT&T ISP topology), with consideration of NACK mechanism on mitigating IFA. Furthermore, some very important results are presented and analyzed.

A. Simulation Description

The final steady state of the exact SIS process in the finite network is the absorbing state [20], because the probability of all infected nodes recovering from the viral state is always larger than zero in the finite network. Actually, the steady state of the NIMFA model corresponds to the meta-stable state in the exact SIS process. The meta-stable state is not clearly defined and hard to detect [20]. Therefore, Li *et al.* [52] proposed to approximate the meta-stable state in the exact SIS process by the steady state in the ε-SIS model [53]. One of the merits of the ε-SIS model is that the introduction of the self-infection Poisson process with rate ε makes it possible to eliminate the absorbing state in the exact SIS process. One only needs to simulate the ε-SIS process for an extremely long time period and calculate the time-average value of the measurement concerned such as the number of infected nodes. Van Mieghem and Cator [53] investigated thoroughly the ε-SIS model and reported that the ε-SIS model could be used to approximate the exact SIS model if a small enough self-infection rate $\varepsilon < \delta/N$ is chosen.

We implement a discrete-time simulator to simulate the ε-SIS model. We begin the simulator by randomly selecting some nodes to be infected. Since we only care about the steady state, the initial infection fraction of nodes does negligible impact on the steady state. The simulator operates step by step in simulation time. At each time step, we calculate the probabilities of each kind of Poisson events. The Poisson events mainly include the self-infection event, the infection event, and the recovering event. For each node i, it is infected by itself with probability $\varepsilon \times (\Delta t)$, where ε and Δt denote the rate of the self-infection Poisson process and the time step, respectively. In this paper, the self-infection rate is the same for each node. For each infected node i, it will get recovered with probability $\delta_i \times (\Delta t)$. For each link $e_{i,j}$ connecting the infected node i and the healthy but susceptible node j, the node j will be infected by the node i with probability $\beta_i \times (\Delta t)$.

At each time step, we record the measurements that we are concerned with, such as the fraction y_∞ of infected nodes. In this paper, we set the value of the time step as 0.001 time unit and run the simulation for 500 time units. After that, we could calculate the time-average value of the number of infected nodes.

B. Complete Topology

The complete topology used for model verification here consists of 40 nodes. In this case, the number of corresponding differential equations is 40, where we solve the systems of differential equations with the help of MATLAB.

To realistically evaluate the effect of IFA on NDN architecture, we set the β_j, δ_i and a_{ij} according to the real conditions in NDN scenario. For example, the TTL for each PIT entry in a router is set to 2 s [25], [26], and the RTT of the Internet is of the milliseconds level [49], [50]. Thus, after normalizing these two parameters at the second level, we set δ_a = 1/2 =0.5, and δ_b = 1/0.05 = 20 (e.g., RTT = 50 ms) in our simulation.

In the simulation setting, all the 40 nodes serve as the routers with the same forwarding capacity (with bandwidth of 100 Mb/s and latency of 5 ms), and each of them connects to a content consumer and producer. According to the work in [54], the choices of different caching polices and cache provisioning methods do little to the relative performance of NDN. Thus, we simply select least recently used as the content caching strategy and uniform cache provisioning for each router in the experiments, to satisfy potential interests with the cached data. In addition, the forwarding strategy of each router is set to the flooding strategy by sending packets to all its out-interfaces, to investigate the damage effect of IFA on NDN at the maximum level, as well as to better characterize the effectiveness of NACK mechanism when suffering such a violent IFA. Furthermore, the PIT entries recording malicious interests in NACK-enabled nodes are evicted at the time-scale of RTT due to the responded NACK messages. However, those PIT entries will be flushed until timeout (the time-scale of TTL of PIT) if the nodes are not implemented with NACK mechanism. That is, the routers/nodes in the given topology are divided into two types, the one with NACK or not. The NACK-enabled node can recover from IFA at the rate of δ_b, while others at the rate of δ_a. The parameter p indicates the fraction of NACK-enabled routers in the topology. We change p to investigate the effect of NACK mechanism on mitigating IFA.

Similar to [18], the initial fraction of infected nodes is set to 10%, that is, $v_i(0) = 0.1$. In each simulation round, four nodes are randomly chosen from the 40 nodes in the given topology

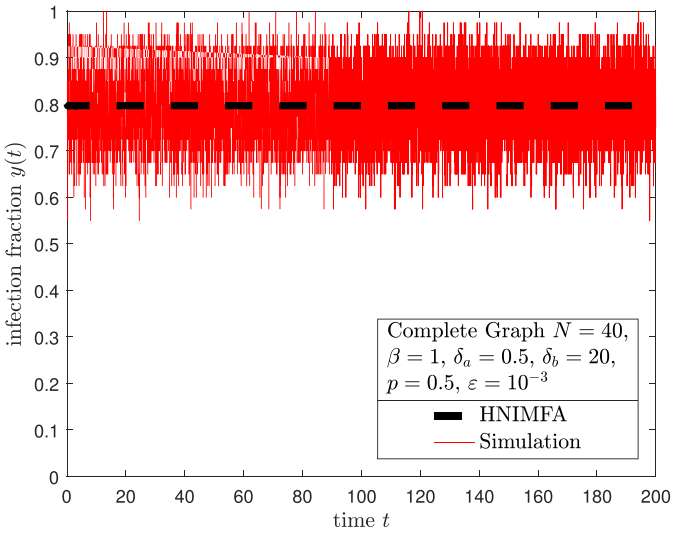

Fig. 1. Infection fraction of NDN routers under metastable state (theoretical model versus simulation).

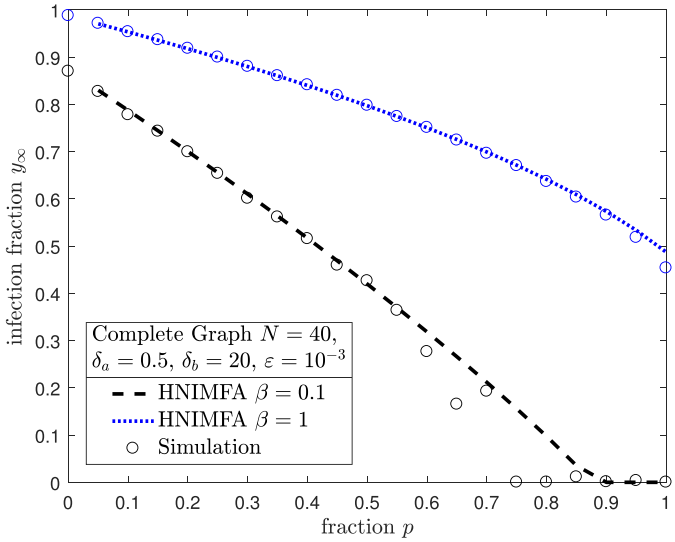

Fig. 2. Infection fraction of the whole network varies with different fractions of NACK-enabled routers.

as the initially infected nodes, occupying 10% of all the nodes. For each infected node, its interest-sending rate is normalized to β interests/s on an average for each of its connected neighbor routers, where the packet sending behavior follows the Poisson distribution. For instance, $\beta = 1$ represents every infected node that sends malicious interests to each of its neighbors at the rate of one interest packet per second on an average.

Fig. 1 demonstrates how the fraction of infected nodes evolves with the simulation time, where the black-dashed line denotes the steady-state infection fraction y_∞ calculated by the proposed HNIMFA model and the red curve denotes the simulation results of the ε-SIS model. It appears that the HNIMFA model can approximate the simulation results well and that the steady-state value is irrelevant to the initial value. Thus, we can use the ε-SIS model (described in Section V-A) to calculate the average metastable state value of the network measurements of the heterogeneous SIS process.

To explore how the fraction of NACK-enabled routers affects the infection fraction of all the NDN routers, we conduct an experiment with varying fraction of NACK nodes, and Fig. 2 shows the corresponding results. In this figure, a higher infection fraction indicates a larger number of NDN routers with their PITs caching malicious interest states, and means more NDN routers suffering the attack of IFA. It can be observed that for different infection rates in the same complete topology, the infection fractions follow the similar pattern. The infection fraction of NDN routers is almost linearly decreased when the fraction of NACK nodes increases. That is, if more NDN routers are implemented with NACK mechanism, the damage of IFA on the NDN architecture can be significantly mitigated, and thus better security can be achieved. This is why we argue to embed the NACK mechanism into the original network protocol stack of NDN. In addition, for the IFA with a smaller infection rate, it can even be totally mitigated with an adoption rate smaller than 100%.

To further investigate the effect of NACK mechanism on NDN's security, we investigate how the infection fraction

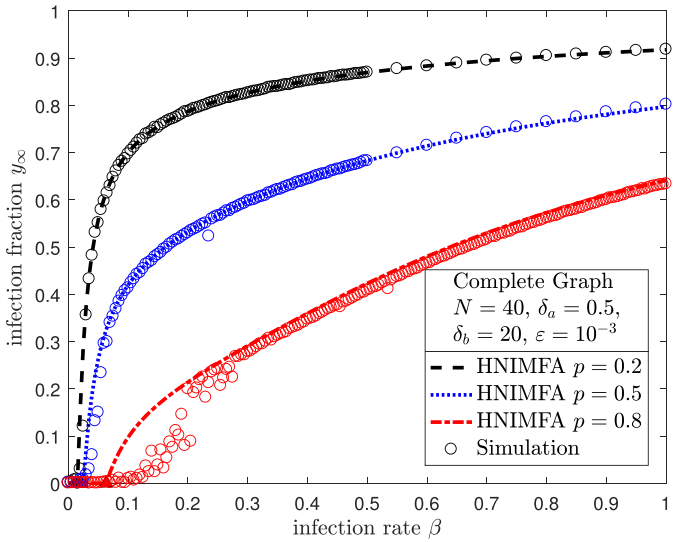

Fig. 3. Relationship of infection fraction and epidemic rate.

changes with varying infection rate, when an IFA launches in scenarios with three different fractions of NACK-enabled routers. As shown in Fig. 3, the infection fraction increases with the infection rate, yet different boost infection rates are needed if different fractions of NACK-enabled routers are implemented in NDN. When the NACK-enabled routers occupy 20% of all the networking devices, the boost infection rate that can bring in real damage is smaller than 0.005. However, if the fraction is increased to 80%, the boost infection rate is almost three times compared with its 20% implementation. In this case, it is much more harder for the IFA to achieve enough damage on NDN architecture.

Furthermore, for the same infection rate such as $\beta = 0.3$, if 80% of NDN routers are implemented with NACK mechanisms, the final infection fraction of the whole network devices is no more than 40%. However, if only 20% of them are implemented

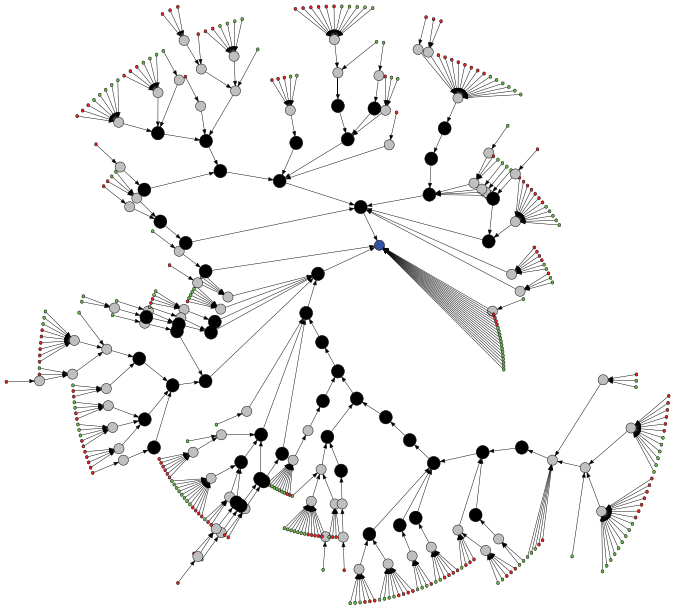

Fig. 4. Rocketfuel's AT&T topology (from our previous work [17]).

TABLE II
LINK SETTINGS OF THE ROCKETFUEL'S AT&T TOPOLOGY

Link type	Delay	Bandwidth
Client-Gateway	$10ms$ - $70ms$	$1Mbps$ - $3Mbps$
Gateway-Gateway	$5ms$ - $10ms$	$10Mbps$ - $20Mbps$
Gateway-Backbone	$5ms$ - $10ms$	$10Mbps$ - $20Mbps$
Backbone-Backbone	$5ms$ - $10ms$	$40Mbps$ - $100Mbps$

with NACK, the infection fraction may significantly increase to bigger than 80%, which means the malicious interest packets sent from the IFA have exhausted 80% of all the NDN routers. That is, most of the network devices are successfully attacked, and thus huge damage can be achieved by launching such an IFA.

Therefore, from the aspect of security, we recommend to enable NACK mechanism in NDN.

C. Realistic Large-Scale Internet Topology

The performance of the proposed theoretical model is also validated in the real Internet topology from AT&T (Rocketfuel's AT&T topology [55]), as shown in Fig. 4.

The parameters β, δ, and $v_i(0)$ are using the same settings as Section V-B. However, the a_{ij} is very different. In this realistic topology, the 625 nodes are divided into three categories: Clients, gateways, and backbones. Nodes are classified to *clients* if they have a degree less than four. Based on this rule, 296 nodes in this topology fall into this type. The nodes are treated as *gateways* if they are directly connected to clients, and 221 nodes belong to this type. Finally, the remaining nodes, with a total of 108, are classified as *backbones*. To simulate as realistic as the Internet in real world, the link bandwidth and delay are set to random values within respective ranges according to their types, as shown in Table II. The content producer is randomly placed at a selected gateway in every run of the simulations.

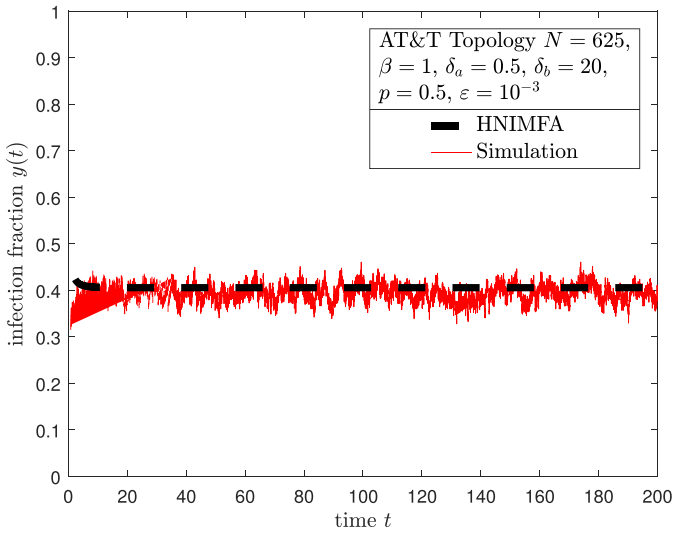

Fig. 5. Infection fraction in metastable state when using realistic large Internet topology (theoretical model versus simulation).

The evaluation results are shown in Fig. 5, where the dash line indicates the theoretical results and the red solid one represents the simulation results. The match of these two results demonstrates the proposed theoretical analyzing model for evaluating the damage effect of IFA in the large-scale and realistic operating network topology. Although the parameter settings here are exactly the same as the experiments in the complete graph, the results are very different when compared with Fig. 1, which indicates that different networking structures can significantly affect the damage effect of the same attack. For instance, the metastable values for infection fraction of the realistic AT&T topology are about 0.4, which is much smaller than 0.8 in the complete graph, when these two types of network topologies suffer from the same IFA and with the same fraction of NACK-enabled NDN routers. This may be because the linking structure of AT&T topology is much more sparse than the complete topology (e.g., less connections between routers), which significantly decreases the epidemic rate of malicious interest packets from the IFA.

Fig. 6 shows that the infection fraction is decreased when more routers are enabled with NACK in the real AT&T topology. However, the decreasing rate is much quicker here than in the complete graph (see Fig. 2), which means the NACK mechanism becomes much more effective on mitigating an IFA when implemented in the realistic Internet topology rather than in the complete graph. This may be because any router in the real Internet has much less connections with its neighbors than in a complete topology, and thus more IFA traffic will travel through this router since less choices can be selected for them when they want to reach a certain victim. In this case, when the NACK mechanism is implemented in this router, more IFA traffic can be filtered. Thus, in this case, the damage effect of IFA can be reduced at a quicker rate accordingly.

Based on the results of Fig. 7, we can deduce that the total number of infected routers by an IFA in the realistic AT&T topology follows similar patterns as in the complete graph, yet

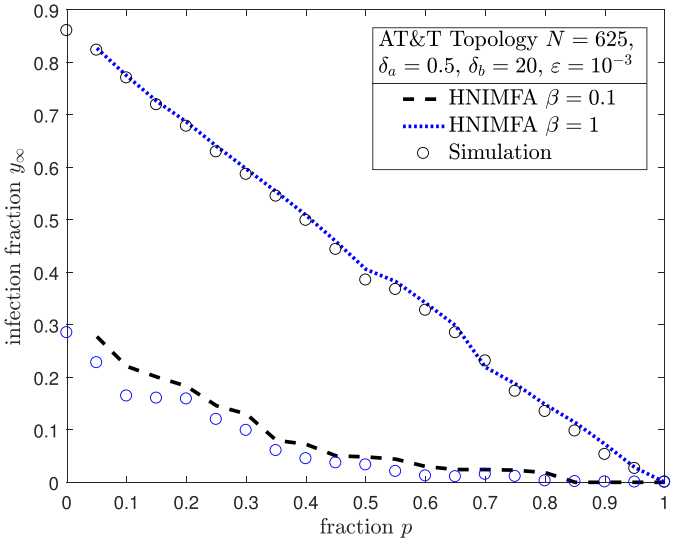

Fig. 6. Infection fraction varies when different fractions of routers are enabled with NACK in a realistic Internet topology.

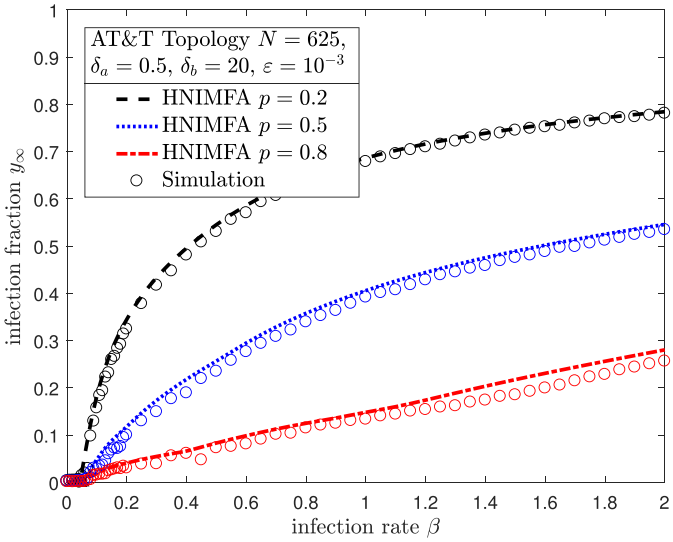

Fig. 7. Infection fraction changes with epidemic rate in the realistic Internet topology.

the final infection fraction in this real Internet topology is slightly smaller than in the complete graph. This may be because the connections between any two nodes in the real Internet is sparser than the complete graph, which brings in more obstacles for an IFA to attack. Furthermore, similar with the conclusions in the complete graph, if more NDN routers are enabled with the NACK mechanism, the infection fraction will be smaller, which indicates better security level. For example, for the IFA with an infection rate $\beta = 1$, if the fraction of NACK-enabled routers is increased from 20% to 80%, the final infection fraction of nodes can be reduced significantly from about 70% to 10%. In this case, much more NDN routers can be saved from this IFA. Based on these analysis, higher adoption rate of NACK can achieve huge security improvement for NDN architecture on mitigating IFA.

VI. Conclusion

The IFA has become one of the most harmful network attacks in NDN architecture, and the consensus has been formed on countering this type of attack. There have been plenty of research works on analyzing its damage on NDN, yet quantitative analysis of NACK on mitigating IFA is neglected in this popular area.

In this paper, a comprehensive category for IFA research is first presented involving the most recently types of new IFA variants as well as state-of-the-art IFA countermeasures. Then, a theoretical analyzing model is designed, which may be the first quantitative analyzing tool to evaluate both the damage effect of IFA and the practical necessity of implementing the interest NACK in NDN. Furthermore, the correctness and availability of the proposed analyzing model are demonstrated by simulations in a complete graph as well as a large-scale and realistic Internet topology. Finally, from both the theoretical analysis and simulations, interest NACK is suggested to be directly implemented into NDN's original protocol stack, if considering from the point of defending IFA to improve the security level of the innovative networking architecture. For instance, increasing the proportion of the NACK implementation in critical routers can raise the epidemic threshold to make IFA traffic more difficult to spread, meanwhile significantly decrease the infection fraction of all the involved routers. That is, more NACK-enabled routers are preferred because they can result in a more enhanced ability to counter the notorious IFA.

In our future work, we will conduct our efforts on how to design a theoretical model to analyze the potential of the blockchain technology on mitigating IFA, and explore possible methods to counter IFA with blockchain-based economic incentive (e.g., trading resources that can be used to defend against attacks [56]). In addition, the structure type of a network may be a significant factor to its invulnerability, since different network topologies can bring very different network security effects [57]. Following this path, building a more invulnerable NDN network by designing the structure of the NACK transmission overlay networks is also one of the important research directions.

References

[1] L. Zhang, "Named data networking," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, pp. 66–73, Jul. 2014.
[2] V. Jacobson, D. K. Smetters, J. D. Thornton, M. Plass, N. Briggs, and R. Braynard, "Networking named content," *Commun. ACM*, vol. 55, no. 1, pp. 117–124, Jan. 2012.
[3] N. Cheng, "Big data driven vehicular networks," *IEEE Netw.*, vol. 32, no. 6, pp. 160–167, Nov./Dec. 2018.
[4] C. Fang, H. Yao, Z. Wang, W. Wu, X. Jin, and F. R. Yu, "A survey of mobile information-centric networking: Research issues and challenges," *IEEE Commun. Surv. Tut.*, vol. 20, no. 3, pp. 2353–2371, Third quarter 2018.
[5] M. Amadeo, C. Campolo, and A. Molinaro, "Information-centric networking for connected vehicles: A survey and future perspectives," *IEEE Commun. Mag.*, vol. 54, no. 2, pp. 98–104, Feb. 2016.
[6] K. Wang, H. Yin, W. Quan, and G. Min, "Enabling collaborative edge computing for software defined vehicular networks," *IEEE Netw.*, vol. 32, no. 15, pp. 112–117, Sep. 2018.
[7] Q.-Y. Zhang, X.-W. Wang, M. Huang, K.-Q. Li, and S. K. Das, "Software defined networking meets information centric networking: A survey," *IEEE Access*, vol. 6, pp. 39 547–39 563, Jul. 2018.

[8] W. Quan, Y. Liu, H. Zhang, and S. Yu, "Enhancing crowd collaborations for software defined vehicular networks," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 80–86, Aug. 2017.

[9] R. Tourani, S. Misra, T. Mick, and G. Panwar, "Security, privacy, and access control in information-centric networking: A survey," *IEEE Commun. Surv. Tut.*, vol. 20, no. 1, pp. 566–600, First quarter 2018.

[10] C. Yi, A. Afanasyev, L. Wang, B. Zhang, and L. Zhang, "Adaptive forwarding in named data networking," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 42, no. 3, pp. 62–67, Jul. 2012.

[11] C. Yi, A. Afanasyev, I. Moiseenko, L. Wang, B. Zhang, and L. Zhang, "A case for stateful forwarding plane," *Comput. Commun.*, vol. 36, no. 7, pp. 779–791, Apr. 2013.

[12] C. Ghali, G. Tsudik, and E. Uzun, "Network-layer trust in named-data networking," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 5, pp. 12–19, Oct. 2014.

[13] Z. Zhang *et al.*, "An overview of security support in named data networking," *IEEE Commun. Magazine*, vol. 56, no. 11, pp. 62–68, Nov. 2018.

[14] D. Smetters and V. Jacobson, "Securing network content," PARC, Tech Rep., pp. 1–7, Oct. 2009. [Online]. Available: https://named-data.net/wp-content/uploads/securing-network-content-tr.pdf

[15] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, "Interest flooding attack and countermeasures in named data networking," in *Proc. IFIP Netw.Conf.*, Brooklyn, NY, USA, 2013, pp. 1–9. [Online]. Available: https://ieeexplore.ieee.org/document/6663516

[16] C. Ghali, G. Tsudik, E. Uzun, and C. A. Wood, "Closing the floodgate with stateless content-centric networking," in *Proc. 26th Int. Conf. Comput. Commun. Netw.*, Vancouver, BC, Canada, 2017, pp. 1–10.

[17] K. Wang, H. Zhou, Y. Qin, J. Chen, and H. Zhang, "Decoupling malicious interests from pending interest table to mitigate interest flooding attacks," in *Proc. IEEE Globecom Workshops*, Atlanta, GA, USA, 2013, pp. 963–968.

[18] W. Yang, Y. Qin, and Y. Yang, "Analysis of malicious flows via SIS epidemic model in CCN," in *Proc. IEEE Conf. Comput. Commun. Workshops*, Honolulu, HI, USA, Apr. 2018, pp. 748–753.

[19] R. Pastor-Satorras, C. Castellano, P. Van Mieghem, and A. Vespignani, "Epidemic processes in complex networks," *Rev. Modern Phys.*, vol. 87, pp. 925–979, Aug. 2015. [Online]. Available: https://link.aps.org/doi/10.1103/RevModPhys.87.925

[20] P. Van Mieghem, J. Omic, and R. Kooij, "Virus spread in networks," *IEEE/ACM Trans. Netw.*, vol. 17, no. 1, pp. 1–14, Feb. 2009.

[21] P. Van Mieghem and J. Omic, "In-homogeneous virus spread in networks," 2014, arXiv:1306.2588.

[22] R. Pastor-Satorras and A. Vespignani, "Epidemic dynamics and endemic states in complex networks," *Phys. Rev. E*, vol. 63, May 2001, Art. no. 066117. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevE.63.066117

[23] E. Cator and P. Van Mieghem, "Second-order mean-field susceptible-infected-susceptible epidemic threshold," *Phys. Rev. E*, vol. 85, May 2012, Art. no. 056111. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevE.85.056111

[24] T. Nguyen *et al.*, "A security monitoring plane for named data networking deployment," *IEEE Commun. Mag.*, vol. 56, no. 22, pp. 88–94, Nov. 2018.

[25] S. Mastorakis, A. Afanasyev, and L. Zhang, "On the evolution of NDNSIM: An open-source simulator for ndn experimentation," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 47, no. 3, pp. 19–33, Jul. 2017.

[26] A. Afanasyev, I. Moiseenko, and L. Zhang, "NDNSIM: NDN simulator for ns-3," NDN, Tech. Rep. NDN-0005, pp. 1–7, Oct. 2012. [Online]. Available: https://named-data.net/wp-content/uploads/TRndnsim.pdf

[27] E. G. AbdAllah, H. S. Hassanein, and M. Zulkernine, "A survey of security attacks in information-centric networking," *IEEE Commun. Surv. Tut.*, vol. 17, no. 3, pp. 1441–1454, Third quarter 2015.

[28] X. Fu, G. Fortino, W. Li, P. Pace, and Y. Yang, "WSNS-assisted opportunistic network for low-latency message forwarding in sparse settings," *Future Gener. Comput. Syst.*, vol. 91, pp. 223–237, Feb. 2019.

[29] A. Compagno, M. Conti, C. Ghali, and G. Tsudik, "To nack or not to nack? negative acknowledgments in information-centric networking," in *Proc. 24th Int. Conf. Comput. Commun. Netw.*, Las Vegas, NV, USA, 2015, pp. 1–10.

[30] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in *Proc. ACM 5th Int. Conf. Emerg. Netw. Exp. Technol.*, Rome, Italy, 2009, pp. 1–12.

[31] S. Signorello, S. Marchal, J. Franois, O. Festor, and R. State, "Advanced interest flooding attacks in named-data networking," in *Proc. IEEE 16th Int. Symp. Netw. Comput. Appl.*, Cambridge, MA, USA, 2017, pp. 1–10.

[32] K. Wang, Y. Zhao, S. liu, and X. Tong, "On the urgency of implementing interest nack into CCN: From the perspective of countering advanced interest flooding attacks," *IET Netw.*, vol. 7, no. 3, pp. 136–140, May 2018.

[33] H. Salah and T. Strufe, "Evaluating and mitigating a collusive version of the interest flooding attack in NDN," in *Proc. IEEE Symp. Comput. Commun.*, Messina, Italy, 2016, pp. 938–945.

[34] F. Guimares, A. Rocha, C. Albuquerque, and I. Ribeiro, "Modeling NDN pit to analyze the limits of timeout on the effectiveness of flooding attacks," in *Proc. IEEE Symp. Comput. Commun.*, Messina, Italy, 2016, pp. 1245–1250.

[35] K. Wang, J. Chen, H. Zhou, Y. Qin, and H. Zhang, "Modeling denial-of-service against pending interest table in named data networking," *Int. J. Commun. Syst.*, vol. 27, no. 12, pp. 4355–4368, Dec. 2014.

[36] J. J. Cochran, L. A. Cox, P. Keskinocak, J. P. Kharoufeh, and J. C. Smith, *The M/G/s/s Queue*, J. J. Cochran, Ed., New York, NY, USA: Wiley, 2010.

[37] Y. Xin, Y. Li, W. Wang, W. Li, and X. Chen, "A novel interest flooding attacks detection and countermeasure scheme in NDN," in *Proc. IEEE Global Commun. Conf.*, Washington, DC, USA, 2016, pp. 1–7.

[38] T. Zhi, H. Luo, and Y. Liu, "A gini impurity-based interest flooding attack defence mechanism in NDN," *IEEE Commun. Lett.*, vol. 22, no. 2, pp. 538–541, Jan. 2018.

[39] Y. Xin, Y. Li, W. Wang, W. Li, and X. Chen, "Detection of collusive interest flooding attacks in named data networking using wavelet analysis," in *Proc. IEEE Mil. Commun. Conf.*, Baltimore, MD, USA, 2017, pp. 557–562.

[40] T. Nguyen, R. Cogranne, and G. Doyen, "An optimal statistical test for robust detection against interest flooding attacks in CCN," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manag.*, Ottawa, ON, Canada, 2015, pp. 252–260.

[41] P. V. Rani, N. Ravi, S. M. Shalinic, and P. Pariuentham, "Detecting and assuaging against interest flooding attack using statistical hypothesis testing in next generation ICN," in *Proc. Int. Conf. Comput., Commun., Signal Process.*, Chennai, India, 2018, pp. 1–5.

[42] K. Wang, W. Bao, Y. Wang, and X. Tong, "Evaluating and mitigating malicious data aggregates in named data networking," *KSII Trans. Internet Inf. Syst.*, vol. 11, no. 9, pp. 4641–4657, Sep. 2017.

[43] K. Wang, H. Zhou, H. Luo, J. Guan, Y. Qin, and H. Zhang, "Detecting and mitigating interest flooding attacks in contentcentric network," *Secur. Commun. Netw.*, vol. 7, no. 4, pp. 685–699, Apr. 2014.

[44] K. Wang, H. Zhou, Y. Qin, and H. Zhang, "Cooperative-filter: Countering interest flooding attacks in named data networking," *Soft Comput.*, vol. 18, no. 9, pp. 1803–1813, Sep. 2014.

[45] R. Shinohara, T. Kamimoto, K. Sato, and H. Shigeno, "Cache control method mitigating packet concentration of router caused by interest flooding attack," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Tianjin, China, 2016, pp. 324–331.

[46] J. Dong, K. Wang, Y. Lyu, L. Jiao, and H. Yin, "Interestfence: Countering interest flooding attacks by using hash-based security labels," in *Proc. Int. Conf. Algorithms Archit. Parallel Process.*, Guangzhou, China, Nov. 2018, pp. 1–8.

[47] G. Liu, W. Quan, N. Cheng, K. Wang, and H. Zhang, "Accuracy or delay? A game in detecting interest flooding attacks," *Internet Technol. Lett.*, vol. 1, no. 2, pp. 1–6, Mar. 2018.

[48] A. Alston and T. Refaei, "Neutralizing interest flooding attacks in named data networks using cryptographic route tokens," in *Proc. IEEE 15th Int. Symp. Netw. Comput. Appl.*, Cambridge, MA, USA, 2016, pp. 85–88.

[49] D. Mirkovic, G. Armitage, and P. Branch, "A survey of round trip time prediction systems," *IEEE Commun. Surv. Tut.*, vol. 20, no. 3, pp. 1758–1776, Third quarter 2018.

[50] S. Khoussi, D. Pesavento, L. Benmohamed, and A. Battou, "NDN-trace: A path tracing utility for named data networking," in *Proc. 4th ACM Conf. Inf.-Centric Netw.*, Berlin, Germany, 2017, pp. 116–122.

[51] H. Dai, Y. Wang, J. Fan, and B. Liu, "Mitigate DDoS attacks in NDN by interest traceback," in *Proc. Conf. Comput. Commun. Workshops*, Turin, Italy, Apr. 2013, pp. 381–386.

[52] C. Li, R. van de Bovenkamp, and P. Van Mieghem, "Susceptible-infected-susceptible model: A comparison of n-intertwined and heterogeneous mean-field approximations," *Phys. Rev. E*, vol. 86, Aug. 2012, Art. no. 026116. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevE.86.026116

[53] P. Van Mieghem and E. Cator, "Epidemics in networks with nodal self-infection and the epidemic threshold," *Phys. Rev. E*, vol. 86, Jul. 2012, Art. no. 016116. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevE.86.016116

[54] S. K. Fayazbakhsh *et al.*, "Less pain, most of the gain: Incrementally deployable ICN," in *Proc. ACM SIGCOMM*, Hong Kong, China, 2013, pp. 147–158.
[55] N. Spring, R. Mahajan, D. Wetherall, and T. Anderson, "Measuring ISP topologies with rocketfuel," *IEEE/ACM Trans. Netw.*, vol. 12, no. 1, pp. 2–16, Feb. 2004.
[56] H. Yao, T. Mai, J. Wang, Z. Ji, C. Jiang, and Y. Qian, "Resource trading in blockchain-based industrial internet of things," *IEEE Trans. Ind. Inform.*, vol. 15, no. 6, pp. 3602–3609, Mar. 2019, doi: 10.1109/TII.2019.2902563.
[57] X. Fu, Y. Yang, and O. Postolache, "Invulnerability of clustering wireless sensor networks against cascading failures," *IEEE Syst. J.*, vol. 13, no. 2, pp. 1431–1442, Jun. 2019, doi: 10.1109/JSYST.2018.2849779.

Kai Wang (M'12) received the B.S. and Ph.D. degrees from Beijing Jiaotong University, Beijing, China.

He is currently an Associate Professor with the School of Computer Science and Technology, Harbin Institute of Technology, Weihai (HIT, Weihai), China. Before joining HIT, he was a Postdoctoral Researcher with Tsinghua University, Beijing, China. He is the Guest Editor of *International Journal of Digital Multimedia Broadcasting*, and Technical Reviewer for many important international journals, such as *ACM Computing Surveys* and IEEE INTERNET OF THINGS JOURNAL. He has authored and coauthored more than 20 papers in prestigious international journals and conferences (e.g., IEEE NETWORK, *ACM Transactions on Internet Technology*, *Information Sciences*). His current research interest includes cyberspace security.

Dr. Wang serves as a Technical Program Committee Member of IPCCC 2018/2019 and a member of China Computer Federation. He is the Deputy Secretary-General of the Blockchain Branch of the Chinese Institute of Electronics.

Dongchao Guo received the Ph.D. degree in signal and information processing from Beijing Jiaotong University, Beijing, China, in 2014.

He is currently an Assistant Professor with the School of Computer Science, Beijing Information Science and Technology University (BISTU), Beijing, China. Before joining BISTU, he was a Postdoctoral Research Fellow with Tsinghua University, Beijing, China. He has authored and coauthored more than ten papers in prestigious international journals (e.g., *Physical Review E*, IEEE NETWORK, *Journal of Physics A*). His current research interest include modeling and analysis of complex networks.

Wei Quan (M'14) received the Ph.D. degree in communication and information system from the Beijing University of Posts and Telecommunications, Beijing, China, in 2014.

He is an Associate Professor with the School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing, China. He has authored and coauthored more than 20 papers in prestigious international journals and conferences including IEEE COMMUNICATIONS MAGAZINE, IEEE WIRELESS COMMUNICATIONS, IEEE NETWORK, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE COMMUNICATIONS LETTERS, *IFIP Networking*, IEEE Wireless Communications and Networking Conference, etc. and serves as an Associate Editor of the *Journal of Internet Technology*, *Journal of Communications and Information Networks*, Guest Editor of *IET Networks,* and as a Technical Reviewer for many important international journals. His research interests include key technologies for network analytics, future Internet, 5G networks, and vehicular networks.

Dr. Quan is also a Technical Program Committee Member of the IEEE International Conference on Communications (2017, 2018), ACM MOBIMEDIA (2015–2017), and IEEE Conference on Cloud Computing and Intelligence Systems (2015 and 2016). He is also a member of ACM and a Senior Member of the Chinese Association of Artificial Intelligence.