A Negotiation-Based Scheme for Interconnecting Heterogeneous Networks With Enhanced Services

Ziqiang Wang, Ke Xu, Guang Cheng, Xiaoliang Wang, Shenglin Jiang, and Yi Cai

Abstract

Although the TCP/IP protocols have made great contributions to the development of the Internet, there is a consensus that the Internet needs improvement to solve the address space exhausted, content-oriented service, and so on. The academic community has proposed lots of valuable but heterogeneous network protocols, which provide better network services but split the Internet. To connect these heterogeneous networks, many middleboxes (*e.g.*, NAT and Tunnel) are deployed on Internet, but these middleboxes mask the communication peers and shield various network services that are provided by these heterogeneous networks. In this paper, we propose the HNN (heterogeneous networks negotiation), which provides transparent end-to-end communication and connects heterogeneous networks stateless in the data plane. What's more, HNN enables the host to perceive the available network service provided by heterogeneous networks and helps the host structure appropriate packet header and packet forwarding path to take advantage of these heterogeneous networks services. We implement and evaluate an HNN prototype with commodity Barefoot Tofino programmable switch S9180-32X. The evaluation results demonstrate that HNN introduces little processing time overhead (no more than 3%) compared to well-known heterogeneous connectivity techniques (*i.e.*, NAT and Tunnel) and allows hosts to utilize heterogeneous network services.

Introduction

The Internet architecture with TCP/IP has achieved great success, which shields the diversity of heterogeneous underlying technologies and supports innovative applications. However, there is a consensus that the current Internet design also has many shortcomings. Such as the IPv4 address space is exhausted, the lack of a security design that has left the Internet vulnerable to a wide range of attacks (*e.g.*, IP address spoofing [1], denial of service [2] and DNS hijacking [3]), and the basic service model of the Internet (point-to-point packet delivery) is not ideally suited to today's network requirements, which are predominantly content-oriented [4].

With these aforementioned shortcomings of the current Internet, the academic community has proposed a lot of valuable schemes. Such as IPv6, SCION [5] and NDN [6]. However, the Internet, almost by design, does not facilitate a clean, incremental path for the adoption of new capabilities at the IP waist [7]. As a result, there are many incompatible heterogeneous networks, which provide various network services with different packet formats. These heterogeneous networks improve network quality of service in some contexts, but split the Internet and hinder the Internet's evolution. Many middleboxes (*e.g.*, NAT and Tunnel) are used to connect these heterogeneous networks and eliminate the deadlock of innovation.

However, these middleboxes have many limitations, such as NAT64 hiding the communication peer and can only initiate the session from one end. What's more, the middlebox techniques shield the services provided by heterogeneous networks and make the host lose the opportunity to benefit from these heterogeneous network services. For example, a host in the IPv4 domain wants to request content and it could only connect to the IPv4 server for this content even though there is an NDN network available on the packet path to the server. This impacts the performance and utilization of the Internet. We seek to find a scheme that enhances the network service by connecting heterogeneous networks with stateless in the data plane and enables hosts to benefit from available heterogeneous network services.

In this paper, we propose the HNN (heterogeneous networks negotiation), which makes the host aware of various heterogeneous network services that are provided by heterogeneous networks. HNN helps the host to construct the appropriate packet header that is used to forward and invoke services in different heterogeneous networks. When a host has some network requirements (*e.g.*, request content), it will send its requirement to the service platform with a negotiation packet first. The negotiation packet carries host's requirement and some packet header parameters. After receiving the negotiation packet, the service platform will combine the host requirement and available heterogeneous network services to determine the packet forwarding

Digital Object Identifier: 10.1109/MNET.114.2100752
Date of Current Version: 16 February 2024
Date of Publication: 13 March 2023

Ziqiang Wang, Guang Cheng (corresponding author), and Shenglin Jiang are with the School of Cyber Science and Engineering, Southeast University, Nanjing 214135, China; Ke Xu and Yi Cai are with the Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China; Xiaoliang Wang is with the Information Engineering College, Capital Normal University, Beijing 100089, China.

direction and add some packet parameters if necessary. Finally, the negotiation packet arrived at a node that can provide the content. This node will return a negotiation reply packet with packet header parameters to the host via service platform. After completing this negotiation process, the communication parties perceive the available network service and get the appropriate packet header construction for invoking the service. Then, the subsequent packets can be forwarded and use the comfortable services in heterogeneous networks smoothly.

We make the following contributions in this paper:

- We propose the HNN, which connects heterogeneous networks stateless in the data plane.
- HNN enables the host to perceive the available network service provided by heterogeneous networks and helps the host construct appropriate network layer header and forwarding paths.
- We connect IPv4, IPv6, and NDN networks with HNN based on the commodity Barefoot Tofino programmable switch S9180-32X to demonstrate the HNN is efficient and beneficial.

In the rest of this paper, we give the HNN detail with an example in II. Then, we implement and evaluate an HNN prototype in III and analyze the challenges and opportunities in V. Finally, we make a conclusion in VI.

The Detailed Description of HNN

In this section, we describe the details of HNN to show how can we connect the heterogeneous networks via negotiation. Firstly, we give an overview of HNN with an example, as shown in Fig. 1. Then we introduce two connection stages in HNN: the heterogeneous networks negotiation stage and the heterogeneous networks connection stage.

A Overview of HNN

Consider a host in an IPv4 domain and proceeds to require a file named "network.org." In the canonical IPv4 network, this host will connect to an IPv4 content server, express its requirement and download this "network.org" file without deliberateness. Because there are no other alternative solutions. However, the Internet has gradually changed and many novel networks (e.g., NDN) have been proposed, deployed, and connected. Even though these heterogeneous networks are simply spliced together with NAT or Tunnel, the current Internet has become a collection of multiple different networks rather than a single IPv4 network. With HNN, the host in IPv4 domain has the opportunity to use other alternative services provided by other heterogeneous networks. As shown in Fig. 1, there is an IPv4 network connection with an IPv6 network and an NDN network. When the host within an IPv4 domain wants to request the "network.org," it will send a negotiation packet that includes its requirement to the service platform first. The platform analyzes this negotiation packet, chooses the best content source (e.g., NDN network), and helps construct the network layer packet header and forwarding path. To be more precise, the negotiation packet will be forwarded from the IPv4 service platform to the NDN service platform. The NDN service platform spread this content requirement in the NDN network and returns a negotiation reply packet. After finishing the negotiation process successfully, the IPv4 host downloads the "network.org" from NDN network with the negotiated packet header. In a nutshell, the host gets the appropriate packet header and forwarding path with the service platform via negotiation stage firstly. Then the host uses the specific packet header to meet its requirement in the connection stage.

> HNN helps the host to construct the appropriate packet header that is used to forward and invoke services in different heterogeneous networks.

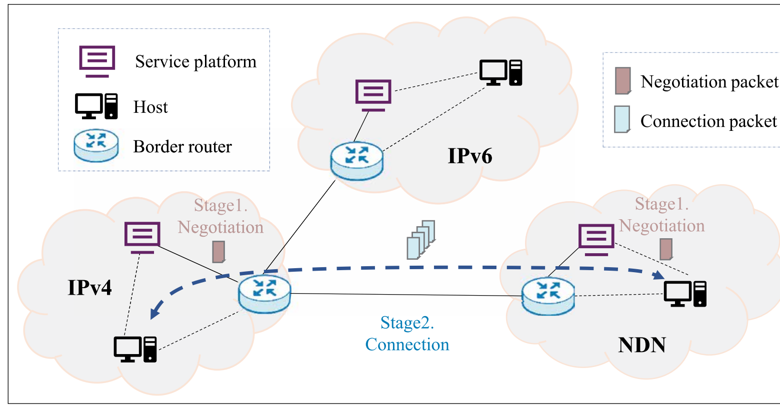

FIGURE 1. An example of HNN, which includes three heterogeneous networks and two stages.

Heterogeneous Networks Negotiation

The heterogeneous network negotiation stage involves communication parties and multiple service platforms. The service platform relies on the border router that connects heterogeneous networks with physical links and is configured with multiple protocol stacks to support parsing various packet headers and collecting heterogeneous network services information. These heterogeneous network services information can be embedded in the extended BGP protocol and propagated to service platforms through border routers. As for the domain with multiple border routers, we deploy the corresponding number of service platforms. These service platforms in the same domain advertise available heterogeneous network service information to each other with the extended IGP protocol.

As for the IPv4 host in our example, it will get the service platform information (e.g., its IPv4 address) when joining the domain through the bootstrapping mechanisms (e.g., DHCP). When this host requires the "network.org" file, it uses the negotiation packet with the service platform to complete the negotiation stage. As shown in Fig. 2, the host sends the negotiation packet that includes a negotiation header and an IPv4 header.

This negotiation packet will be transited to the service platform via internal routers, which perform IPv4 packet forward logic. After the service platform received this negotiation packet, it parses the packet and finds the requirement is getting a file named "network.org." This platform weighs the available heterogeneous network service (*i.e.*, IPv4 content server, IPv6 content server, and NDN network) and chooses the NDN network.[1] Then the service platform adds an NDN header over this negotiation packet and forwards it to the NDN network. The NDN network service platform will continue to process this negotiation packet and spread the requirement in the NDN network. Finally, this negotiation packet arrives at an NDN node that has this file. This NDN node will return a negotiation reply packet to the IPv4 host through service platforms. The negotiation reply packet processing is similar to the negotiation packet. After the IPv4 host received the negotiation reply packet, the negotiation stage is completed. The communication parties cache the packet header and forwarding path that is carried in the negotiation packet or negotiation reply packet, then turn into the stable connection stage.

Heterogeneous Networks Connection

In the heterogeneous network connection stage, the communication parties use the appropriate packet header, which is structured by service platforms, to transmit data during heterogeneous networks smoothly. We take transmitting the "network.org" file as an example. The NDN node parses the negotiation packet, which includes an NDN header, an IPv4 header, and a negotiation header. It learns that the appropriate network layer packet header is an NDN header covering an IPv4 header and transmits data with this mixed packet header (as shown in Fig. 3). We refer to this type of packet as the connection packet. In the NDN domain, the connection packet is forwarded with the NDN header. When this

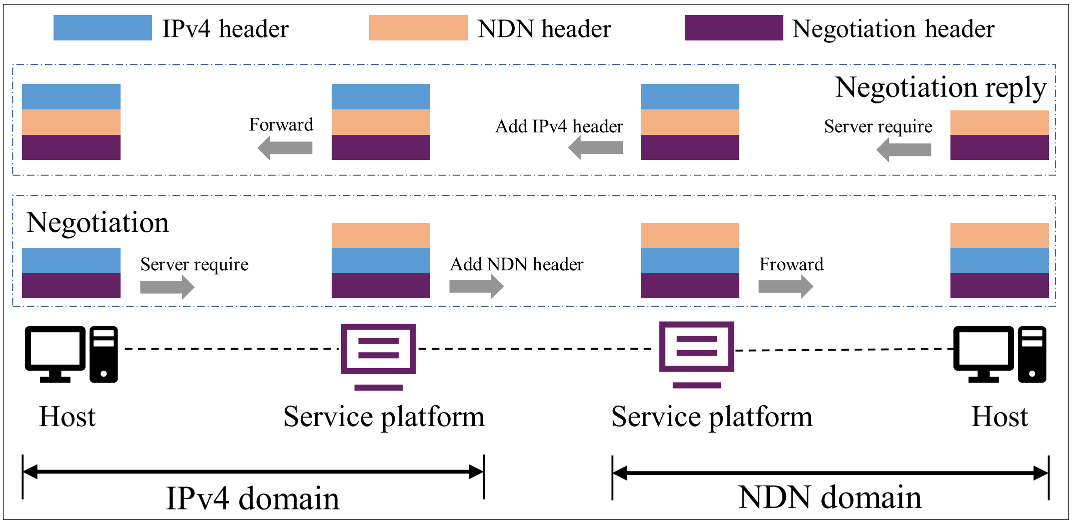

FIGURE 2. The heterogeneous networks negotiation stage. Hosts express their service requirements with negotiation or negotiation reply packets. Upon receiving a negotiation or negotiation reply packet, the service platform will parse the service requirement, add a new L3 packet header (if need), and forward it.

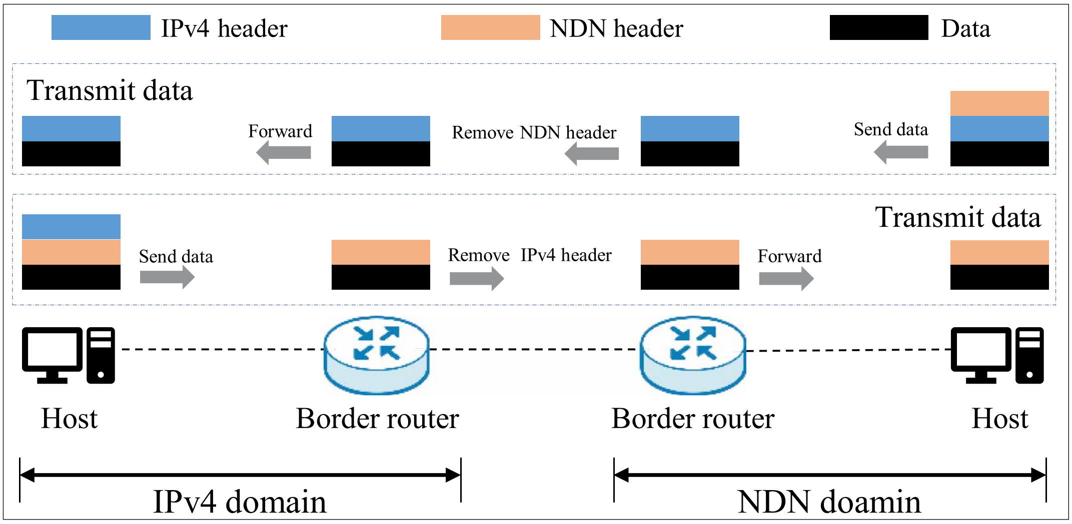

FIGURE 3. The heterogeneous network connection stage. Hosts transmit data using the mixed header structured by service platforms. When receiving a connection packet, which does not have the negotiation header, the border router will forward it and remove the outermost L3 packet header (if need).

[1] Generally, the NDN network is more suitable for content distribution. Here also can use smarter algorithms to compare services and choose the best.

connection packet reaches the border router, the border router strips its NDN header to expose the IPv4 header and forward it to the IPv4 domain. Finally, this connection packet arrives at the IPv4 host based on its IPv4 header. During the connection stage, the router is stateless and focuses on forwarding packets besides removing some packet headers on the border router.

Implementation

We implement a prototype HNN with the commodity Barefoot Tofino programmable switch S9180-32X and set the service platform on the switch control plane.

A Draft of HNN Header

In our HNN prototype, we implement the negotiation packet with insert a slim negotiation header between L3 and L4, as shown the brown part in Fig. 4.

Our negotiation header consists of five parts. The version part (4 bits), nHdr part (4 bits), and total length part (8 bits) are the common header descriptions. The flag part (4 bits) indicates the type of negotiation packet: the negotiation request packet with the flag is 0 and the negotiation reply packet with the flag is 1. The request ID is used to distinguish between different negotiation processes on the same host and the negotiation reply packet must take the correct request ID otherwise this negotiation reply packet should be considered invalid and discarded. As for the host requirement and header parameters, we put them in the payload part which will be parsed and handled in the service platform and host.

Component Description

Host: We take three ubuntu 18.04 hosts as the communication parties that use HNN protocol to connect together through IPv4, IPv6, and NDN networks. Each host runs the negotiation protocol to send and handle the negotiation request/reply packet in the heterogeneous networks negotiation stage. The host will assign a unique ID number to each negotiation process and set it in the negotiation packet header. After finishing the negotiation stage, each host caches the header structure and forwarding path of the mixed packet. Then they use the connection packet to transmit data through heterogeneous networks.

Border Router: The border router connects at least two heterogeneous networks and supports parsing these heterogeneous packets. There are two packet handle logic in the border router, as for the negotiation packet, which includes negotiation request or reply packet header, the border router should send it to the heterogeneous network port based on its L3 header if its ingress port is not the control port, otherwise send it to the control plane. For packets without negotiation header, the border router first performs general network layer forwarding, such as IP address longest prefix matching, and then determine whether to remove the outermost L3 header according to the forwarding port.

Service Platform: We implement this service platform on the programmable switch control plane. The service platform handles the negotiation packet according to the available heterogeneous network services. After receiving a negotiation packet, the platform parses its payload and gets the host requirement. Then it chooses the appropriate heterogeneous network service, adds a new L3 header and forwards this packet. In our HNN prototype, we preconfigure the heterogeneous network service information in the service platform.

Evaluation

We set three hosts in IPv4, IPv6, and NDN networks respectively, and connect these three heterogeneous networks through the service platform. The host can perceive the available heterogeneous network services through the service platform and select the appropriate network service with HNN. Here, we evaluate the performance of the negotiation stage which mainly involves service platform processing and the performance of the connection stage that forwards the connection packet on the border router. Precisely, we evaluate the packet processing time when the IPv4 host connects with an IPv6 host, requires the content from NDN and the IPv6 host requires the content from NDN.

As for the negotiation stage, we conducted 1000 experiments to test the service platform processing time and analyze the impact of the negotiation stage on network performance. The results are shown in Fig. 5, from which it can be found that more than 80% of the negotiation packet is completed within 25ms. The average negotiation time for IPv4-IPv6, IPv4-NDN, and IPv6-NDN on the service platform is 23.508ms, 22.517ms, and 23.646ms, respectively. This negotiation process time will increase if more complex decision algorithms are used. But it should note that the negotiation process is only triggered when establishing a new connection and we argue that this negotiation time overhead is acceptable.

After completing the negotiation stage, the host uses the connection packet for heterogeneous network communication. This connection packet contains the specified header structure which determines the forwarding path and service mode. The forwarding process of connection packets does not involve the service platform but removes the outermost network layer headers one by one on the heterogeneous network border routers. We evaluate the forwarding time overhead of the connection packet on the heterogeneous network border router with various size payloads (*i.e.*, 126 Bytes, 768

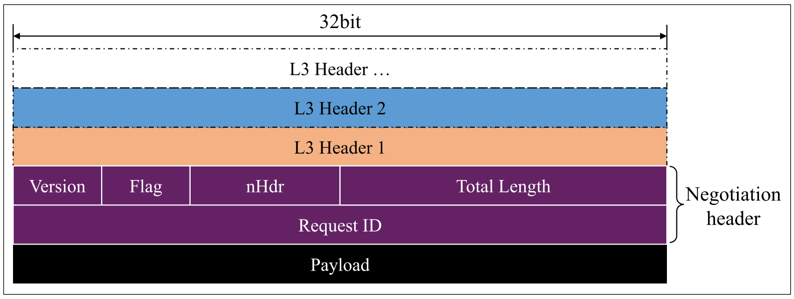

FIGURE 4. A draft of the HNN header, which is a slim customized header between L3 and L4.

Many heterogeneous networks are gradually deployed to improve the user experience separately and there is a significant functional gap between them.

Bytes, and 1500 Bytes) and the result is shown in Fig. 6a. It can be found that the forwarding time in different scenarios is stable because the border router just removes the outermost L3 packet header and forwards the packet. What's more, we compare the forwarding time overhead of connection packets with some well-known network technologies (*i.e.*, IPv4, IPv6, NAT, and Tunnel) using the 768 Bytes payload. As can be seen from Fig. 6b, the processing time overhead on the heterogeneous network border routers is larger than simple IP packet forwarding, but this extra time overhead is only on the border router. The processing time overheads of NAT, tunnel, and HNN are 731.53, 728.76, and 750.5 nanoseconds, respectively. The network performance of HNN is comparable to the existing heterogeneous network splicing technology (*e.g.*, NAT and Tunnel) and enables the host to use various heterogeneous network services. Therefore we argue that HNN is beneficial and competitive.

Challenges and Opportunities

There is a widespread agreement that the current Internet is both inherently flawed and deeply entrenched [4]. The IP protocol is deeply embedded in host networking and application software, as well as in router hardware and software. Therefore, the Internet changes face extremely high deployment barriers (as evinced by the decades-long effort to move from IPv4 to IPv6). Many heterogeneous networks are gradually deployed to improve the user experience separately and there is a significant functional gap between them. An advisable scheme is connecting these heterogeneous networks and enabling the host to benefit from heterogeneous network services. In this paper, we propose the HNN that connects heterogeneous networks exquisitely via negotiation and there are maybe some challenges when deploying HNN in the current Internet. We analyze these challenges and present some solutions in this section.

Select the Appropriate Heterogeneous Network Service. The current Internet is complicated and unstable. More specifically, the network congestion and routing failures are common occurrences on the Internet. The heterogeneous networks are more uncontrollable and

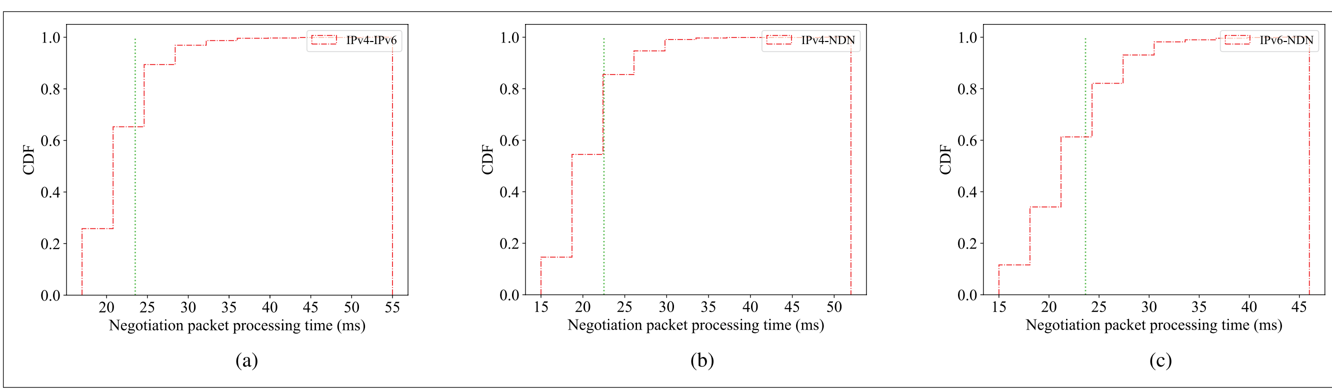

FIGURE 5. Negotiation process time overhead on the service platform. a) Negotiate IPv4 and IPv6. b) Negotiate IPv4 and NDN. c) Negotiate IPv6 and NDN.

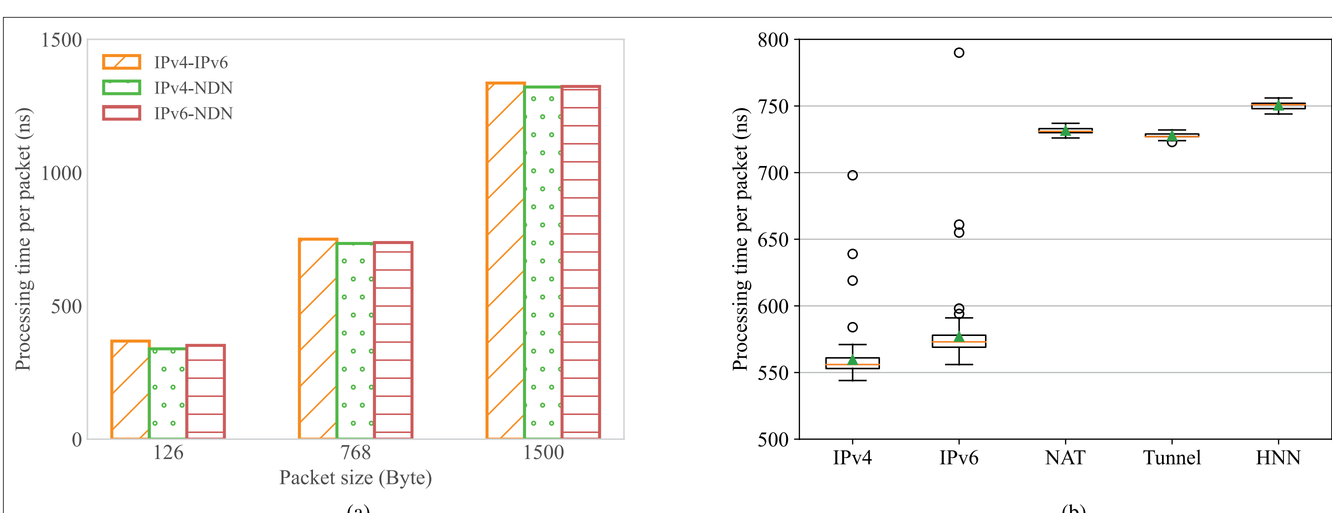

FIGURE 6. Packet forwarding time overhead on border router. a) Forwarding time overhead of different size connection packets. b) Forwarding time overhead for multiple network technologies.

the network link states have a great impact on the quality of service. Choosing the appropriate network service to meet the host requirement in the fickle heterogeneous networks is tricky. The service platform needs to evaluate these heterogeneous network services with link states dynamically. Fortunately, there are already some inter-domain link-state sharing strategies available for reference [8]. We can add some heterogeneous network link states in the BGP protocol and enable the service platform to select appropriate services dynamically.

The Heterogeneous Network Negotiation With Massive Flows. The heterogeneous network negotiation in the service platform will introduce some overhead, especially using some intelligent complex algorithms to evaluate and select the appropriate heterogeneous network services. Considering the massive traffic forwarded on the backbone network equipment, take the negotiation with such scale flows on the backbone service platform will be stressful. We recommend using distributed negotiation. To be precise, the backbone border router only focuses on data plane forwarding and distributes the heterogeneous network service information to its subnetworks. The heterogeneous network negotiation stage is completed with the service platforms in the subnetworks.

Incremental Deployment the Service Platform. Every change to the Internet does not happen overnight and we need to improve the Internet gradually. Fortunately, the HNN can be deployed incrementally. When some domains have deployed the HNN, then they can share heterogeneous network services and better meet host requirements immediately. The available heterogeneous network services will increase with the gradual deployment of HNN. The exciting thing is that with the development of NFV (Network Functions Virtualization) [9], [10], [11] and SDN (Software Defined Network) [12], [13], [14], we can implement the service platform as a virtual network function and modify the border router expediently.

The Security Considerations About HNN. Internet is notoriously hard to secure. Although our main purpose is to connect heterogeneous networks and allow hosts to benefit from diverse heterogeneous network services, we do not want to introduce security risks with HNN. The negotiation with the service platform is important and determines the subsequent communication process of the host. The sophisticated attacker may impersonate the service platforms, hijack the negotiation packets and then manipulate host communications to inject malicious code or steal sensitive data. We recommend deploying a packet filtering mechanism on border routers. More precisely, a domain should discard negotiation packets from outside and the source address is the service platform of this domain. In addition, we also recommend that the service platform be certified with RPKI [15] to ensure that the negotiation process is conducted via the legitimate service platforms. Since the negotiation packets are only used at the beginning of the session, we argue that these security mechanisms related to the negotiation stage do not impose too much burden on the network.

The negotiation with the service platform is important and determines the subsequent communication process of the host.

Conclusion

The Internet has flourished and solidified for decades. However, the innovation and evolution of the Internet infrastructure itself are difficult. The reason could be attributed to the inability of the fixed Internet architecture to accommodate innovations in core mechanisms, such as the inability to dynamically deploy a non-IP addressing model better suited to content-oriented scenarios. As a result, many heterogeneous network services were deployed to enhance the Internet separately and the Internet gradually became a collection of many isolated networks.

In this paper, we propose the HNN that enhances the network services via connecting the heterogeneous networks with negotiation. We aim to enable hosts to perceive and benefit from the various heterogeneous network services provided in the Internet. Combined with the development status of the Internet, we try to change the Internet infrastructure as little as possible. Therefore, we complete the heterogeneous network negotiation stage through some service platforms deployed on the network edge, which is the origin of the evolution because each edge network is by nature a single management domain and has a clean interface with external networks. These service platforms coordinate various heterogeneous network services and better meet the host requirements via negotiation. We demonstrate that it is feasible to connect heterogeneous networks smoothly through negotiation with an HNN prototype.

Acknowledgment

This work was supported in part by the National Key Research and Development Program of China under Grant 2022YFB3102301; in part by the China National Funds for Distinguished Young Scientists under Grant 61825204; in part by the NSFC Project under Grant 61932016, Grant 62132011, and Grant 62132009; and in part by the Beijing Outstanding Young Scientist Program under Grant BJJWZYJH01201910003011.

References

[1] M. Luckie et al., "Network hygiene, incentives, and regulation: Deployment of source address validation in the Internet," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2019, pp. 465–480.

[2] Q. Yan et al., "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 602–622, 1st Quart., 2016.

[3] V. C. Perta et al., "A glance through the VPN looking glass: IPv6 leakage and DNS hijacking in commercial VPN clients," in *Proc. Privacy Enhancing Technol.*, 2015, pp. 77–91.

[4] J. McCauley et al., "Enabling a permanent revolution in Internet architecture," in *Proc. ACM Special Interest Group Data Commun.*, 2019, pp. 1–14.

[5] X. Zhang et al., "SCION: Scalability, control, and isolation on next-generation networks," in *Proc. IEEE Symp. Secur. Privacy*, May 2011, pp. 212–227.

[6] L. Zhang et al., "Named data networking (NDN) project," Xerox Palo Alto Research Center-PARC, Palo Alto, CA, USA, Relatório Técnico NDN-0001, 2010, pp. 157–158.

[7] D. Han et al., "XIA: Efficient support for evolvable Internetworking," in *Proc. 9th USENIX Symp. Netw. Syst. Design Implement. (NSDI)*, 2012, pp. 309–322.
[8] S. Previdi et al., *Border Gateway Protocol—Link State (BGP-LS) Extensions for Segment Routing BGP Egress Peer Engineering*, document RFC 9086, 2021, pp. 1–15.
[9] H. Hawilo et al., "NFV: State of the art, challenges, and implementation in next generation mobile networks (vEPC)," *IEEE Netw.*, vol. 28, no. 6, pp. 18–26, Nov./Dec. 2014.
[10] B. Li et al., "ClickNP: Highly flexible and high performance network processing with reconfigurable hardware," in *Proc. ACM SIGCOMM Conf.*, 2016, pp. 1–14.
[11] J. G. Herrera and J. F. Botero, "Resource allocation in NFV: A comprehensive survey," *IEEE Trans. Netw. Service Manag.*, vol. 13, no. 3, pp. 518–532, Sep. 2016
[12] F. Hu, Q. Hao, and K. Bao, "A survey on software-defined network and OpenFlow: From concept to implementation," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 2181–2206, 4th Quart., 2014.
[13] M. Alsaeedi, M. M. Mohamad, and A. A. Al-Roubaiey, "Toward adaptive and scalable OpenFlow-SDN flow control: A survey," *IEEE Access*, vol. 7, pp. 107346–107379, 2019.
[14] R. Amin, M. Reisslein, and N. Shah, "Hybrid SDN networks: A survey of existing approaches," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3259–3306, 4th Quart., 2018.
[15] R. Bush, *Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI)*, document RFC 7115, 2014.

Biographies

Ziqiang Wang is pursuing the Ph.D. degree with the School of Cyber Science and Engineering, Southeast University supervised by Prof. Ke Xu and Prof. Jianping Wu. His research interests include network architecture and security.

Ke Xu (Senior Member, IEEE) received the Ph.D. degree from Tsinghua University, Beijing, China. He is currently a Full Professor with the Department of Computer Science and Technology, Tsinghua University. He has published more than 200 technical papers and holds 11 U.S. patents in the research areas of nextgeneration Internet, blockchain systems, the Internet of Things, and network security. He is a member of ACM. He has guest edited several special issues for IEEE and Springer journals.

Guang Cheng (Senior Member, IEEE) (chengguang@seu.edu.cn) received the B.S. degree in traffic engineering from Southeast University in 1994, the M.S. degree in computer application from the Heifei University of Technology in 2000, and the Ph.D. degree in computer network from Southeast University in 2003. He is a Full Professor with the School of Cyber Science and Engineering, Southeast University, Nanjing, China. His research interests include network security, network measurement, and traffic behavior analysis.

Xiaoliang Wang received the Ph.D. degree from the Department of Computer Science and Technology, Tsinghua University, in 2017. He is currently a Lecturer with the Information Engineering College, Capital Normal University. His research interests include wireless networks and network security.

Shenglin Jiang is currently pursuing the master's degree from the School of Cybersecurity, Southeast University. His research interests include cybersecurity and future network architecture.

Yi Cai is currently pursuing the master's degree with the Department of Computer Science and Technology, Tsinghua University, supervised by Prof. Ke Xu. His research interests include network architecture and security.