Resilience evaluation of multi-path routing against network attacks and failures

Journal Article

Author(s):
An, Hyok; Na, Yoonjong; Lee, Heejo; Perrig, Adrian

Publication date:
2021-06

Permanent link:
https://doi.org/10.3929/ethz-b-000488131

Rights / license:
Creative Commons Attribution 4.0 International

Originally published in:
Electronics 10(11), https://doi.org/10.3390/electronics10111240

electronics

MDPI

Article

Resilience Evaluation of Multi-Path Routing against Network Attacks and Failures

Hyok An [1], Yoonjong Na [1], Heejo Lee [1,*] and Adrian Perrig [2]

[1] Department of Computer Science and Engineering, Korea University, Seoul 02841, Korea; anhyok@korea.ac.kr (H.A.); nooryyaa@korea.ac.kr (Y.N.)
[2] Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland; adrian.perrig@inf.ethz.ch
* Correspondence: heejo@korea.ac.kr

Abstract: The current state of security and availability of the Internet is far from being commensurate with its importance. The number and strength of DDoS attacks conducted at the network layer have been steadily increasing. However, the single path (SP) routing used in today's Internet lacks a mitigation scheme to rapidly recover from network attacks or link failure. In case of a link failure occurs, it can take several minutes until failover. In contrast, multi-path routing can take advantage of multiple alternative paths and rapidly switch to another working path. According to the level of available path control, we classfy the multi-path routing into two types, first-hop multi-path (FMP) and multi-hop multi-path (MMP) routing. Although FMP routing supported by networks, such as SD-WAN, shows marginal improvements over the current SP routing of the Internet, MMP routing supported by a global Internet architecture provides strong improvement under network attacks and link failure. MMP routing enables changing to alternate paths to mitigate the network problem in other hops, which cannot be controlled by FMP routing. To show this comparison with practical outcome, we evaluate network performance in terms of latency and loss rate to show that MMP routing can mitigate Internet hazards and provide high availability on global networks by 18 participating ASes in six countries. Our evaluation of global networks shows that, if network attacks or failures occur in other autonomous systems (ASes) that FMP routing cannot avoid, it is feasible to deal with such problems by switching to alternative paths by using MMP routing. When the global evaluation is under a transit-link DDoS attack, the loss rates of FMP that pass the transit-link are affected significantly by a transit-link DDoS attack, but the other alternative MMP paths show stable status under the DDoS attack with proper operation.

Keywords: network security; multi-path routing; high availability; Internet-scale evaluation

check for updates

Citation: An, H.; Na, Y.; Lee, H.; Perrig, A. Resilience Evaluation of Multi-Path Routing against Network Attacks and Failures. *Electronics* **2021**, *10*, 1240. https://doi.org/10.3390/electronics10111240

Academic Editor: Victor A. Villagrá

Received: 15 April 2021
Accepted: 19 May 2021
Published: 24 May 2021

1. Introduction

1.1. Motivations

The Internet was not designed to maintain high availability in the face of malicious activities. Recent patches to improve Internet security and availability have been constrained by the current Internet architecture design. As network-based attacks on availability continue to increase each year [1], an improvised Internet architecture should offer availability and security based on its design, provide incentives for deployment, and consider economic, political, and legal issues at the design stage [2].

Currently, the Internet provides single path (SP) routing, which lacks a rapid mitigation mechanism to counter Internet hazards, such as network congestion, link failures, or DDoS attacks. Under network congestion or DDoS attacks, the performance of the Internet, such as latency or loss rate, is highly affected, and, in the case of a link failure, it can take several minutes until failover [3]. Fault recovery of the border gateway protocol (BGP) at times takes several minutes before the routes converge to a consistent form [4]. Path outages even lead to significant disruptions in communication, which may last tens of minutes or longer [5–7]. However, if such a network congestion or network failure occurs from a link that an autonomous system (AS) cannot handle, sophisticated operations or cooperation among AS administrators will be required. Detailed routing information is maintained only within a single AS. The information shared with other providers and ASes is heavily filtered and summarized using BGP running at the border routers between ASes [8].

1.2. Multi-Path Routing Approaches

Many approaches have been proposed to solve the problem from network attacks and failures using concepts of multiple paths. A link failure can occur in several ways, such as through natural hazards or by a DDoS attack. In multihoming [9], a network is connected to multiple providers and uses its own range of addresses. If one of the links fails, the protocol recognizes the failure and reconfigures its routing tables. Although multihoming provides a way to connect multiple providers, it is not a multi-path routing but rather an SP routing because we cannot select the connection to the providers for every communication instantly. Resilient overlay networks (RON) [10] are a remedy for potential problems, such as BGP's fault or path outages, because BGP hides information about traffic conditions and topological details in the interests of scalability and policy enforcement. RON can often find paths between its nodes, even while wide-area Internet routing protocols, such as BGP, cannot. This RON approach is an overlay network that selects different waypoints, but it cannot select the actual network path. Multi-path TCP (MPTCP) is the de-facto standard multi-path transport protocol [11]. MPTCT can only make use of a single path per local network interface and, therefore, does not permit path choice as in MMP.

Software Defined WANs (SD-WAN) is a multi-path approach that can mitigate these problems by providing multiple routing paths from the first hop. However, if network congestion or a link failure occurs in other hops through a hazard or adversary that a victim AS cannot control, the SD-WAN will be unable to deal with the problem as it the SD-WAN has no control over other such hops, which can be described as the first type of multi-path routing, first-hop multi-path (FMP) routing. Figure 1 contrasts fully disjoint and partially disjoint paths. In Figure 1a, source AS *Src* has two links—one to next AS A_1, and the other to AS A_2. The AS following A_1 and A_2 is AS *B*. Source AS *Src* has two paths to destination AS *Dst*. However, the two paths use the same links between AS *B* to AS *Dst*. These paths can be disconnected by only one link, that is, link *B*-*C* or *C*-*Dst*. Figure 1b shows the non-overlapping paths from *Src* to *Dst*. As we can see, we cannot guarantee that the given paths are non-overlapped if the paths are established only by source AS's link selection. The second type of multi-path routing is multi-hop multi-path (MMP) routing, which can take advantage of controlling the paths available between a source and a destination. MMP can change to an alternative path to mitigate the problem, if hazards or attacks occur in other hops that a victim AS cannot control. However, to implement MMP on the current Internet architecture, a redesign of the Internet architecture is required.

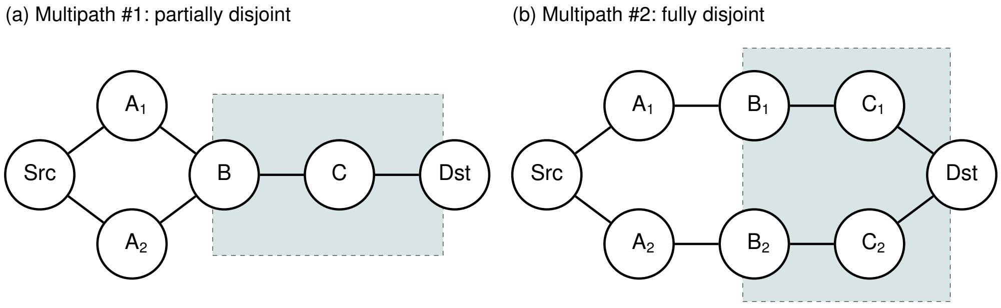
(a) Multipath #1: partially disjoint
A1
Src
B
C
Dst
A2
(b) Multipath #2: fully disjoint
A1
B1
C1
Src
Dst
A2
B2
C2

Figure 1. Source AS *Src* has two links to next hop ASes A_1 or A_2 but (**a**) shows partially disjoint paths that the multi-paths between *Src* and *Dst* uses same links from AS *B* to AS *Dst*, which can be disconnected by a single link failure, whereas (**b**) shows fully disjoint paths that cannot be disconnected by a single link failure.

1.3. Objectives

We classify multi-path routing to be of two types—FMP and MMP—based on path control and verify that the effectiveness of multi-path with real networks deployed globally, especially MMP routing, shows more resilience than FMP used currently. MMP routing enables changing to alternate paths to mitigate the network problem in other hops, which cannot be controlled by FMP routing. In this study, we evaluated the network performance in terms of latency and loss rate [12].

These results indicate that MMP can mitigate a DDoS attack of a transit-link and provide high availability on a global network using scalability, control, and isolation on next-generation networks (SCION) [13,14]. SCIONLab [15,16] is a global research network used to test SCION. We can join the SCION network using our own computation resources and set up and run our own ASes. An AS will actively participate in routing in a SCIONLab network and enable realistic experimentation using the unique properties of the SCION architecture. We conducted an evaluation of multi-path selection on the MMP and compared it with FMP. For a global evaluation, we used a SCIONlab network with nodes from six countries, that is, the United States, Switzerland, Germany, the Republic of Korea, Singapore, and Japan, and considered 18 SCION ASes. For a multi-path test, we assume that there is an attacker attempting to consume the entire bandwidth for communication. To compare MMP with FMP, a situation is assumed in which heavy traffic occurs among the ASes affecting both links configured for SD-WAN, but which cannot be controlled by it.

1.4. Contributions

The contributions of our study are threefold:

1. We classify multi-path routing to be of two types—FMP and MMP—based on path control. Because SP routing lacks rapid mitigation mechanisms to counter Internet hazards, FMP routing can mitigate these problems by selecting a connection link to the first hop beyond its control. However, it cannot deal with a problem in another hop. To mitigate this, MMP routing can take advantage of controlling all paths available between a source and a destination.
2. We verify that the effectiveness of multi-path with real networks deployed globally, especially MMP routing, shows more resilience than FMP used currently. Using the global network, we show that FMP mitigates certain cases of network problems, but MMP gains impressively lower loss rate by comparison.
3. When the global evaluation is under a transit-link DDoS attack, the loss rates of FMP that pass the transit-link are affected significantly by a transit-link DDoS attack, but the other alternative MMP paths show stable status under the DDoS attack with proper operation under 1% loss rates. Meanwhile, the impact to loss rate of FMP is over 40% by a bandwidth of 700 Mbps.

2. Background and Related Work

2.1. Link Failure and Transit-Link DDoS Attack

A link failure can occur in several ways, such as through natural hazards or a DDoS attack. Rerouting is one solution for such a case. Unlike a traditional DDoS attack, Comelt [17] or CrossFire [18] have shown that, by attacking only the core links, an adversary can effectively degrade the victim's network connectivity or cause it to fail using only a small number of resources. Such DDoS attacks are difficult for a victim to detect because their targets are usually several hops away from the victim's AS and are typically not controllable by the victim. However, if a DDoS attack or a link failure occurs from a link that a victim AS has no control over, rerouting from a traditional Internet environment would be a challenge.

2.2. Multihoming

In multihoming [9], a network is connected to multiple providers and uses its own range of addresses. The edge routers of the network communicate with the providers using a dynamic routing protocol, typically BGP. BGP announces its own network address range to all providers. If one of the links fails, the protocol recognizes the failure and re-configures its routing tables. Multihoming requires the use of an address space that is accepted by all providers and causes an increase in the global routing table. Although multihoming provides a way to connect multiple providers, it is not a multi-path routing but rather an SP routing because we cannot immediately select the connection to the providers for every communication.

2.3. Multi-Path Routing

Multi-path TCP (MPTCP) is the de-facto standard multi-path transport protocol [11]. MPTCT can only make use of a single path per local network interface and, thus, does not permit path choise as in MMP. The partial-reliability extension of the stream control transmission protocol (PR-SCTP) offers a primitive the possibility to define a lifetime parameter [19,20]. Liu et al. [21] used linear programming to evaluate multi-path routing from a traffic engineering perspective. Although PR-SCTP offers multihoming capabilities, additional IP addresses are used as a backup in the case of a failure; thus, PR-SCTP is not a fully multi-path protocol and does not address the problem that we describe in this paper [22].

In Reference [23], the authors consider the problem of routing data over multiple disjoint paths and propose a framework for multi-path routing in mobile ad hoc networking (MANET). In Reference [24], they develop an analytical framework for evaluating multi-path routing, and Reference [25] shows the Secure Message Transmission (SMT) protocol, which safeguards the data transmission against arbitrary malicious behavior of other nodes in MANET. Recently, flying ad hoc networks (FANETs) are rapidly proliferating and leading the emergence of the Internet of Drones and its applications. Reference [26] proposes a jamming-resilient multi-path routing protocol, also called JarmRout so that intentional jamming and disruption or isolated and localized failures do not interrupt the overall network performance of FANETs. The JarmRout is designed based on a combination of three major schemes, which are link quality scheme, traffic load scheme, and spatial distance scheme, to select maximally spatial node-disjoint multiple paths with high link quality and light traffic load to deliver the data packets from an source to destination nodes. In our paper, we focus on multi-path for the global network, not the local network.

2.4. Cognitive Packet Network

The Cognitive Packet Network (CPN) is a Quality of Service (QoS)-driven routing protocol, in which each flow specifies the QoS metric (e.g., delay, loss, jitter, or other composite metrics) that it wishes to optimize [27]. The work describes an experimental system that implements multi-path routing. In Reference [28], the authors show how such multi-path routing schemes can be used to mitigate and block network attacks, and in Reference [29] the dynamic recovery and QoS robustness of multi-path routing schemes is demonstrated in the presence of attacks. Reference [30] addresses one of the challenges of multi-path policies in that they create transients in multi-hop systems. In the recent papers by Reference [31,32], the use of multi-path routing to mitigate and recover from attacks with the help of software defined networking (SDN) controllers is discussed, and demonstrated with experimental results. The work in Reference [33] details how SDN controllers can be exploited together with their dynamic ability to vary paths for given connections, to optimize the access to Fog services. The SDN system in the test-bed was extended using the “cognitive packet routing algorithm” [34]. In our paper, we condider and discuss SD-WAN as WAN of SDN on multi-path for the global network.

2.5. SD-WAN: Software Defined WANs

SDN continues to attract both industry and research communities as a modern paradigm for the management and operation of computer networks. SDN is changing how computer networks are managed by providing a centralized network management. SDN separates the control plane of the network with different devices providing a centralized view of the network from the data plane [35]. Conceptually, SDN supports large-scale network control with simple operations and is a new method for preventing network-based attacks [36].

SD-WAN is the combination of a group of network technologies (overlay, performance routing, and firewalling) that uses software to make a WAN more intelligent, flexible, and easier to manage. The key benefits of a SD-WAN are flexibility and intelligence. SD-WAN is an overlay that enables the use of different underlays, i.e., the Internet, MPLS, VPLS, and LTE. For customers building a SD-WAN over the Internet, they can choose their best partner in a location-by-location manner. This also means that customers can mix the underlays and inherit their key benefits, such as the reliability of MPLS and the low cost of Internet access. SD-WAN solutions have been designed from scratch with the application being the key object to manipulate. Thus, monitoring, prioritization, and routing use applicative parameters in their policies and are fully orchestrated. SD-WAN policies, parameters, and topologies are centrally managed in real-time.

The quality of SD-WAN depends on the underlays: for multinational customers looking for savings on their access budget, and thus considering the low-cost last-mile of the Internet, the user experience may be impacted. Because SD-WAN cannot control what happens between selected Internet service providers (ISPs), customers may even lose connections between sites for minutes or even hours. Furthermore, SD-WAN solutions are not interoperable, and customers are vendor-locked. SD-WAN is a growth relay for equipment vendors, system integrators, and service providers and is a way for the cloud service providers to get closer to their customers. Typically, SD-WANs are operated using intra-domain routing protocols.

2.6. Resilient Overlay Networks

RON [10] is a remedy for potential problems, such as BGP's fault or path outages, because BGP hides information about traffic conditions and topological details in the interests of scalability and policy enforcement. Distributed applications layer a "resilient overlay network" over the underlying Internet routing substrate. The nodes comprising a RON reside in a variety of routing domains and cooperate with each other to forward data on behalf of any pair of communicating nodes in the RON. Because ASes are independently administrated and configured, and routing domains rarely share interior links, they generally fail independently of each other. As a result, if the underlying topology has physical path redundancy, RON can often find paths between its nodes, even when wide-area routing Internet protocols, such as BGP, cannot. This RON approach is an overlay network which selects different way-points, but it cannot select the actual network path.

2.7. BGP Poisoning

BGP poisoning is a rerouting technique used in BGP. By using BGP poisoning, an AS can change the routing path that it has no control over. Instead of multi-path routing, BGP poisoning can be another solution for hazards or attacks occurring in an AS that the administrator has no control. For example, Nyx uses BGP poisoning as a countermeasure for a link failure, and LIFEGUARD uses BGP poisoning to recover from a routing failure [37,38]. However, BGP poisoning is not a standard technique. BGP poisoning can also be used as an offensive method, such as BGP hijacking [39].

2.8. SCION Multi-Path Routing Architecture

SCION is the first clean-slate Internet architecture designed to provide route control, failure isolation, and explicit trust information for end-to-end communication. SCION organizes existing ASes into groups of independent routing planes, called isolation domains (ISD), which interconnect to provide global connectivity. Isolation domains provide natural isolation of the routing failures and misconfigurations, give endpoints strong control for both inbound and outbound traffic, provide meaningful and enforceable trust, and enable scalable routing updates with a high path freshness. As a result, the SCION architecture provides strong resilience and security properties as an intrinsic consequence of its design. In addition to high security, SCION also provides a scalable routing infrastructure, and efficient packet forwarding.

As a path-based architecture, SCION end hosts learn about available network path segments, and combine them into end-to-end paths that are carried in the packet headers. Path construction embedded cryptographic mechanisms are constrained to the route policies of the ISPs and receivers, offering a path choice to all parties, i.e., senders, receivers, and ISPs. This approach enables path-aware communication, an emerging trend in networking. These features also enable multi-path communication, which is an important approach for high availability, rapid failover in the case of network failures, increased end-to-end bandwidth, dynamic traffic optimization, and resilience to DDoS attacks [14]. SCION enables a native network-wide multi-path routing, allowing traffic differentiation based on latency and the bandwidth requirements, i.e., latency-critical traffic can be sent over the satellites, and the remaining traffic can be forwarded on a terrestrial network, thus improving the cost-effectiveness of the system [40].

3. Problem Statement

Network congestion occurs owing to traffic-based bandwidth consumption. Congestion is caused by malicious attackers or flash crowds [10] of innocent users. Under network congestion, that is, when the performance of the Internet, including the latency or loss rate, is highly affected by a hazard or when a link failure occurs, it can take several minutes or more until failover [3]. Fault recovery of BGP at times takes several minutes before the routes converge to a consistent form [4]. Path outages even lead to significant disruptions in communication lasting tens of minutes or longer [5–7].

3.1. Single Path or Multi-Path Routing

Multihoming, SD-WAN and SCION appear to be multi-path approaches when viewed we simply look at them as a topology because it is feasible to make multiple connections to other ASes using them. However, if we consider them in terms of routing, each approach operates differently. For clarity, we define here the meanings of SP, FMP, and MMP, including their major differences from the routing mechanism of multihoming, SD-WAN, and SCION.

3.1.1. Single Path (SP)

SP routing is provided by the current Internet architecture. It lacks rapid mitigation mechanisms to counter Internet hazards, such as network congestion or link failures. For example, multihoming is connected to multiple providers, and the edge routers of the network communicate with the providers using a dynamic routing protocol. If one of the links fails, the protocol re-configures its routing tables for a new single path.

3.1.2. First-Hop Multi-Path (FMP)

FMP routing can mitigate these problems by selecting a connection link to the first hop. However, if network congestion or a link failure occurs in another hop, it cannot deal with the problem because the SD-WAN does not have the authority to control the path in the other hops. For example, SD-WAN is an overlay with the ability to use different underlays, that is, the Internet, MPLS, VPLS, and LTE. Because SD-WAN cannot control all that is happening between the selected internet service providers (ISPs), customers may even lose connections to sites for minutes or even hours.

3.1.3. Multi-Hop Multi-Path (MMP)

MMP routing can control all paths available between a source and a destination. This is a crucial approach to high availability, rapid failover in the case of network failures, increased end-to-end bandwidth, dynamic traffic optimization, and resilience to

DDoS attacks. SCION enables native network-wide multi-path routing, allowing traffic differentiation based on latency and bandwidth requirements.

3.2. Types of Multi-Path Routing: FMP and MMP

Although FMP and MMP are not directly comparable, SD-WAN offers application-aware properties (DPI, encryption, and firewalling) that can also be used with SCION. However, SCION offers a super-set of SD-WAN properties at the underlay level: enhanced path selection, trust in the network, and real end-to-end control (not only the first hop). As the core difference, MMP is a public global Internet infrastructure with end-to-end control, whereas FMP providers typically build private networks within the first hop (see Figure 2). An MMP customer can obtain a connection from any ISP offering MMP, whereas an FMP customer is typically locked to one provider (Though there exist certain alliances, it is definitely not an open network). Typically, SD-WANs are operated using intra-domain routing protocols.

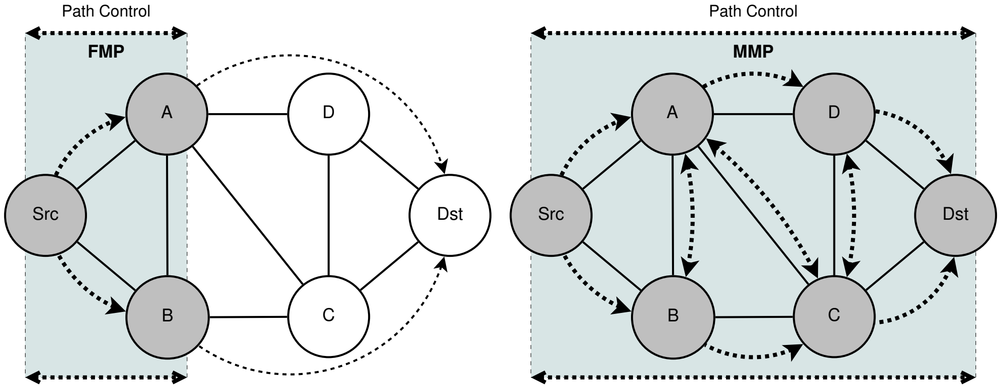

Figure 2. Source AS *Src* can choose a link between/among first hops to mitigate a link congestion/failure; however, FMP cannot choose a path after the first hops even if there are network hazards before the destination *Dst*. MMP can control all ASes between *Src* and *Dst*, allowing a path to be chosen by considering the link status.

It is, therefore, possible to distinguish FMP for one customer controlled using SD-WAN from MMP for any customer in a network dynamically controlled through a public infrastructure, such as SCION. SCION has a much more powerful multi-path routing. For instance, consider the case of a customer with an AS who has a regular Internet connection and an SD-WAN connection. The SD-WAN system can then send a packet over one of two connections. However, a single SCION Internet connection can enable 10 or more paths (depending on the topology) between the source and destination. The path p_n list without the routing loop in Figure 2 is shown below.

- p_0: $Src \rightarrow A \rightarrow B \rightarrow C \rightarrow Dst$
- p_1: $Src \rightarrow A \rightarrow B \rightarrow C \rightarrow D \rightarrow Dst$
- p_2: $Src \rightarrow A \rightarrow C \rightarrow Dst$
- p_3: $Src \rightarrow A \rightarrow C \rightarrow D \rightarrow Dst$
- p_4: $Src \rightarrow A \rightarrow D \rightarrow Dst$
- p_5: $Src \rightarrow A \rightarrow D \rightarrow C \rightarrow Dst$
- p_6: $Src \rightarrow B \rightarrow A \rightarrow C \rightarrow Dst$
- p_7: $Src \rightarrow B \rightarrow A \rightarrow C \rightarrow D \rightarrow Dst$
- p_8: $Src \rightarrow B \rightarrow A \rightarrow D \rightarrow Dst$
- p_9: $Src \rightarrow B \rightarrow A \rightarrow D \rightarrow C \rightarrow Dst$
- p_{10}: $Src \rightarrow B \rightarrow C \rightarrow Dst$
- p_{11}: $Src \rightarrow B \rightarrow C \rightarrow D \rightarrow Dst$
- p_{12}: $Src \rightarrow B \rightarrow C \rightarrow A \rightarrow D \rightarrow Dst$

3.3. Path Establishment against Link Failures on SCION

Since SCION forwarding paths are static, they collapse when one of the links fails. Link failures are handled by a three-pronged approach that typically masks link failures without any outage to the application and rapidly re-establishes fresh working paths [13]:

- Beaconing periodically establishes new working paths.
- SCION control message protocol (SCMP) (SCION-equivalent of ICMP) is used for path-segment revocation. Failed links result in the rapid erasure of affected path segments from path servers.
- SCION end hosts use multi-path communication by default, thus masking link failures to an application with another working path. As multi-path communication can increase availability (even in environments with very limited path choice [10]), SCION beacon servers actively attempt to create disjoint paths, SCION path servers make an effort to select and announce disjoint paths, and end hosts compose path segments to achieve maximum resilience to path failure. Consequently, we expect that most link failures in SCION will be unnoticed by the application, unlike the frequent (although mostly brief) outages in the currently available Internet [38,41].

4. Evaluation

Figure 3 shows a part of the world map (Background world map designed by Layerace/Freepik.) with the nodes used to measure the effectiveness of FMP and MMP on SCIONLab, which deploys SCION on research networks. The core ASes are placed at Carnegie Mellon University in the United States, Magdeburg in Germany, SWISSCOM (SCMN) in Switzerland, NUS in Singapore, and KISTI Daejeon in Korea. We evaluate network performance in terms of latency and loss rate [12].

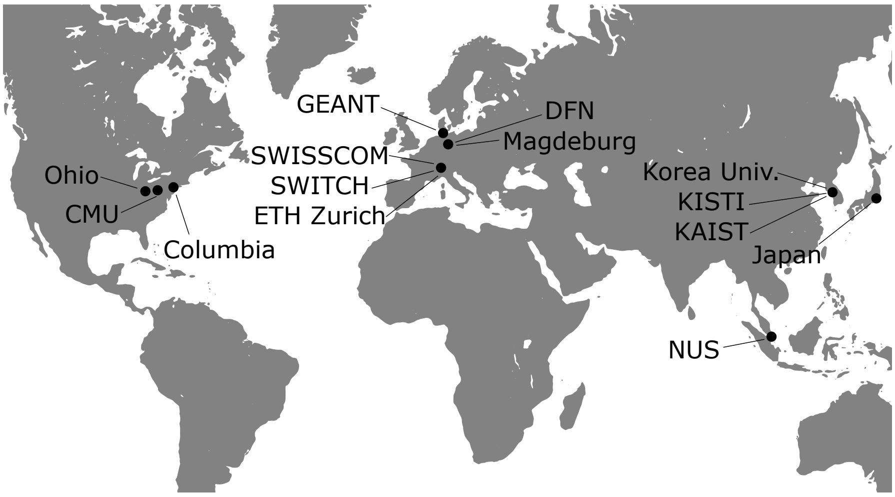

Figure 3. The nodes used for the evaluation with the 6 participating countries including 18 participating SCION ASes. Some dots have several nodes. The nodes *Ohio* and *Japan* are deployed on Amazon Web Services (AWS).

To evaluate latency and loss rate, we employ the SCION ICMP (SCMP) testing tool and SCION bandwidth testing tool provided by SCIONLab [15]. We generate normal/heavy traffic adopting the routing policies of SP, FMP, and MMP on the SCION protocol. The results of the evaluation show proper operation for each routing policy. Under the attack using the heavy traffic, the background ongoing traffic of the network is very small compared to the heavy traffic, and it is enough to be ignored to see the results. This evaluation does not cover the whole cases of the multi-path but it shows the point of comparison for the main characteristics among SP, FMP, and MMP routing.

Initially, for comparison with SP, FMP, and MMP, we select six SCION ASes between Korea and Switzerland. Next, to test the effectiveness of MMP at the Internet-scale during a transit-link DDoS attack, we test using a larger topology with 6 countries and 18 SCION ASes participating in it. During this test, we select four core ASes (the United States, Germany, Switzerland and Korea) from four different countries and set the transit-link between the core ASes as direct path selected countries as shown in Figure 4. We then use these transit-links and measure the loss rate of the paths between the countries.

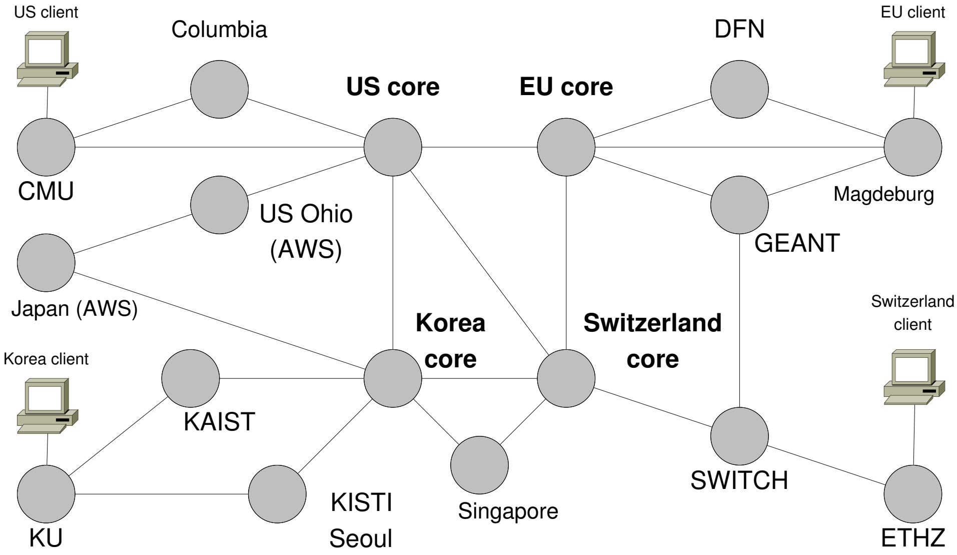

Figure 4. Global topology using SCIONLab for a real-world network evaluation. The core ASes are placed at Carnegie Mellon University (CMU) in the United States (US), Magdeburg in Germany, SWISSCOM (SCMN) in Switzerland, NUS in Singapore, and KISTI Daejeon in Korea. The links between the core ASes are operated as a transit-link for communication. All links are adopted as multi-path to show the effectiveness of MMP. The ETHZ node includes two ASes.

As shown in Figure 5, six ASes are involved between the source *Src* and destination *Dst* for real Internet evaluation between Switzerland and Korea. *A*, *B*, *C*, *D*, *E*, and *F* ASes indicate KU, KISTI Seoul, KAIST, KISTI Daejeon (KR core AS), CMU (US core AS), and SCMN (Switzerland core AS), respectively. There are two links between *F* and *Dst*. After then, we use given global networks to show effectiveness of multi-path routing under high latency.

4.1. Assumptions

We assume that a normal user from the source node *Src* is communicating with the destination node *Dst*. We assume that the usual latency or loss rate of the default routing path is lower than other alternative paths. For a multi-path test, we assume that an attacker consumes the bandwidth of the path that the victim is currently using, making it difficult for the victim to communicate by degrading the network performance, such as through latency increase or packet loss. In this case, we assume that the attacker knows the path setting of the router because in a legacy router protocol, the path setting is pre-configured with a single path. In addition, we assume that an attacker is a passive attacker that cannot recognize when the victim has changed its path.

4.2. Comparison between SP, FMP and MMP Routing

An evaluation of utilization of multiple available MMP paths is also applied to compare the performance using two and four paths, which are written as a multi-path above. In Figure 5, the path $p_0 = \{Src \rightarrow A \rightarrow B \rightarrow D \rightarrow F \nearrow Dst\}$ between *Src* and *Dst* shows under heavy traffic of the communication.

- p_0 = $\{Src \rightarrow A \rightarrow B \rightarrow D \rightarrow F \nearrow Dst\}$: A low-latency path that will be under heavy traffic of communication.

- $p(SP) = \{Src \rightarrow A \rightarrow B \rightarrow D \rightarrow E \rightarrow F \nearrow Dst\}$: A high-latency path that will initially be used as a single path.
- $p(FMP) = \{Src \rightarrow A \rightarrow C \rightarrow D \rightarrow F \searrow Dst\}$: A low-latency path that will be partially affected by an attack.
- $p(MMP) = \{Src \rightarrow A \rightarrow C \rightarrow D \rightarrow E \rightarrow F \searrow Dst\}$: A high-latency path that will mostly be unaffected by an attack.

As aforementioned, FMP cannot deal with network congestion or a link failure if the problem occurs in other hops that FMP cannot control. However, because MMP can take advantage of a path that an FMP, such as SD-WAN, cannot control, MMP can mitigate the problem if such a situation occurs. Figure 5 shows the topology uses for an evaluation towards comparison between FMP and MMP under such a situation. We assume that AS A, which controls the source, uses SD-WAN, and, because an SD-WAN configuration through cooperation with other ASes is difficult, we also assume that the SD-WAN does not control the path passing other AS hops. We use $p(SP)$, $p(FMP)$, and $p(MMP)$ as the path of SP, FMP, and MMP routing.

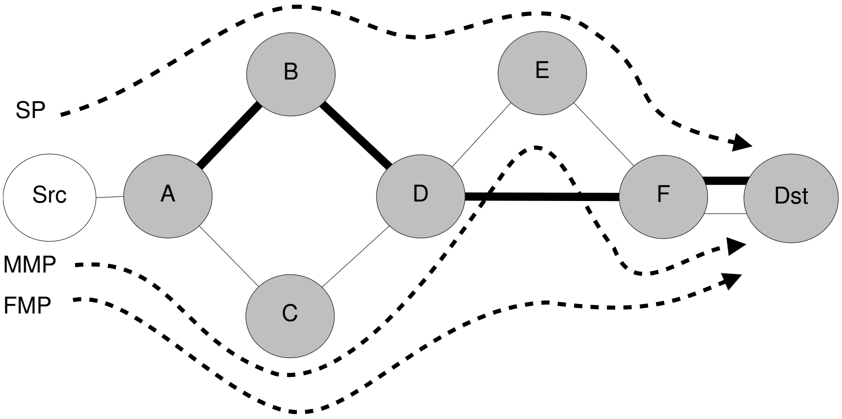

Figure 5. Topology used for comparison between MMP and FMP. The solid bold line indicates heavy traffic. The scenario is a case in which the traffic congestion affects both paths of FMP and MMP, whereas the alternative path found by MMP does not.

If traffic congestion occurs in path $\{A \rightarrow B \rightarrow D\}$, path $\{D \rightarrow F\}$, and path $\{F \nearrow Dst\}$, then both links configured for SP and FMP will suffer a degradation in network performance even though SD-WAN switches its link from a SP path $p(SP)$ to an FMP path $p(FMP)$, or vice versa. However, when it comes to $p(MMP)$, it can be used as an alternative option because MMP can control the path outside the source AS. Because path $\{A \rightarrow C \rightarrow D\}$, path $\{D \rightarrow E \rightarrow F\}$, and path $\{F \searrow Dst\}$ are unaffected by traffic congestion, using this $p(MMP)$, we can mitigate the network performance degradation.

Figure 6 and Table 1 show the results of the network performance of each path $p(x)$ when x is SP, FMP or MMP, under traffic congestion. If traffic congestion occurs on the $p(x)$ mentioned previously, $p(SP)$ and $p(FMP)$, which are options for SD-WAN, will suffer from degraded network performance with an average increase in latency of approximately 46% (SP: 270 ms to 396 ms) and 31% (FMP: 318 ms to 419 ms), and a loss rate of 4.7% and 4%, respectively. However, for the $p(MMP)$, which is an alternative path that can be configured using MMP, the network suffers from almost no network performance degradation.

Table 1. Average latency and loss rate with *FMP paths* and *MMP path* during attack.

Path	Loss Rate	Avg. Latency
$p(SP)$	4.7%	396.66 ms
$p(FMP)$	4%	419.19 ms
$p(MMP)$	0%	318.73 ms

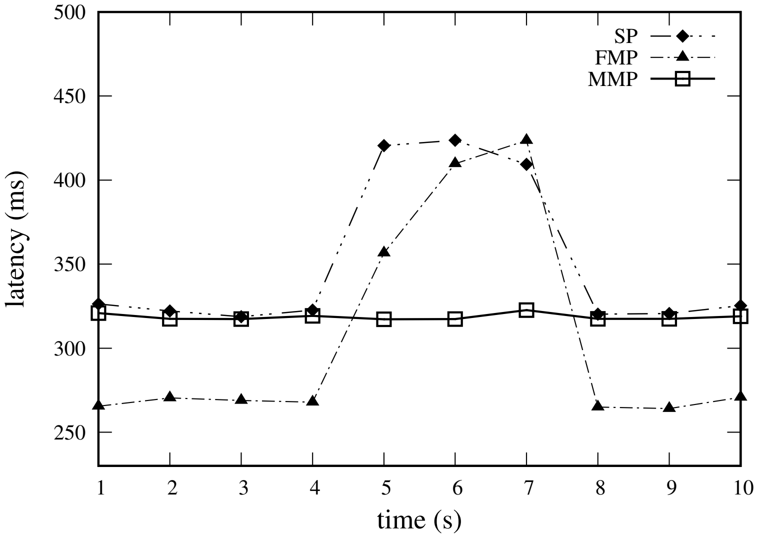

Figure 6. Latency comparison of FMP and MMP when traffic congestion occurs during 4–7 s. Both paths of SP and FMP are affected, whereas the alternative path that MMP found is unaffected.

4.3. Single Path and Concurrent Multi-Path

An evaluation of utilization of multiple available MMP paths is also applied to compare the performance using two and four paths, which are written as a multi-path above. In Figure 7, the node *Src* uses the path $p_0 = \{Src \rightarrow A \rightarrow B \rightarrow D \rightarrow F \nearrow Dst\}$ for communication as an SP routing. For two paths, we used p_0 and p_3, and, for four paths, we used p_0 to p_3 as explained below:

- $p_0 = \{Src \rightarrow A \rightarrow B \rightarrow D \rightarrow F \nearrow Dst\}$: A low-latency path that will initially be used by *Src* as a single path. An attacker will directly attack this path during communication.
- $p_1 = \{Src \rightarrow A \rightarrow C \rightarrow D \rightarrow F \searrow Dst\}$: A low-latency path that will be partially affected by an attack.
- $p_2 = \{Src \rightarrow A \rightarrow C \rightarrow D \rightarrow E \rightarrow F \nearrow Dst\}$: A high-latency path that will be partially affected by an attack.
- $p_3 = \{Src \rightarrow A \rightarrow C \rightarrow D \rightarrow E \rightarrow F \searrow Dst\}$: A high-latency path that will mostly be unaffected by an attack.

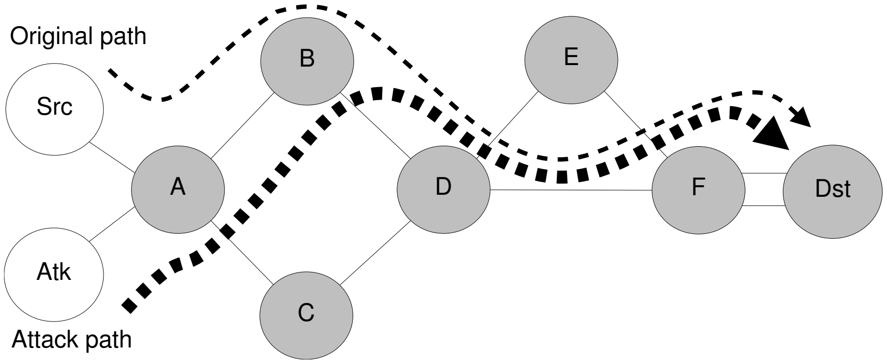

Figure 7. Topology used for MMP evaluation. Dotted curved line shows the user's communication path and the bold dotted line shows the attacker's attack path.

Figure 8 and Table 2 show the results of the comparison when using two paths and four paths for MMP. The paths are selected uniformly at random for the case of '2 paths (random)' and '4 paths (random)'. We sent SCMP packets for 1 s each during a 10 s period (for a total of 10 packets), which consumed the bandwidth for 3 s (from seconds 4 to 7). Because the network status changes owing to the bandwidth consumption of an attacker, selecting stable paths will ensure a much more stable communication with high availability than selecting paths at the same ratio. Here, '4 paths (weighted)' represents selecting 4-times more stable paths than the paths being attacked, and '4 paths (random)' corresponds to randomly selecting all four paths.

The loss rate and average latency of a single path are greater than those obtained using 'MMP: 2 paths (random)' and 'MMP: 4 paths (random)'. Moreover, when using 'MMP: 4 paths (random)', the performance is less affected by an attack with only an approximate 10% increase in the average latency than when using 'MMP: 2 paths (random)' during a bandwidth consumption attack (4–7 s), which shows an increased average latency of approximately 20%. In addition, although the latency showed an improvement, the loss rate shows almost no change because other paths (p_1 and p_2) used for 'MMP: 4 paths (random)' evaluation already encountered a loss rate even when no attack takes place.

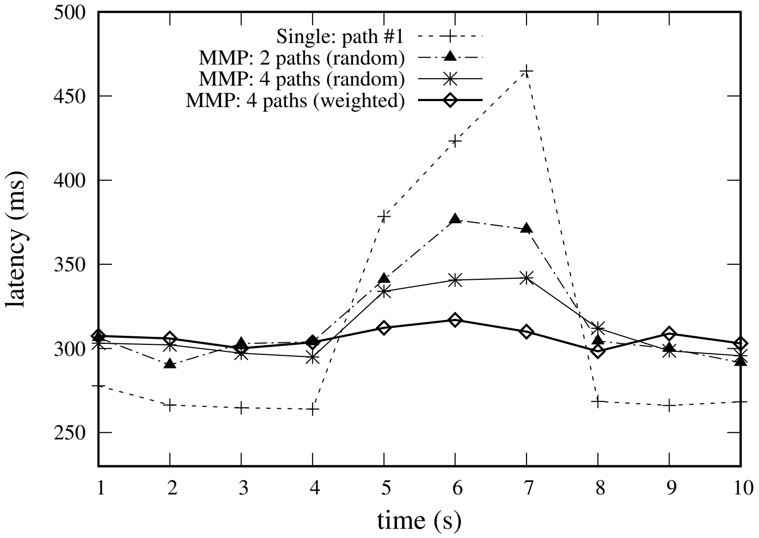

Figure 8. Latency comparison of SP and MMP routing. 'MMP 4 paths' (weighted/random) demonstrates selecting stable paths 4 times more than others and equally selecting all 4 paths by an attack (4–7 s).

Table 2. Experimental results of an SP and MMP for the measurement of loss rates and latency during the attack.

Path	Loss Rate	Avg. Latency
SP: 1 path	7.5%	422.22 ms
MMP: 2 paths (random)	3%	362.77 ms
MMP: 4 paths (random)	3%	330.09 ms
MMP: 4 paths (weighted)	0.5%	313.07 ms

As observed in Figure 8, 'MMP: 4 paths (weighted)' using four times more stable paths mitigate the effect of an attack (during seconds 4 to 7) compared with 'MMP: 4 paths (random)' at the same ratio, because a *weighted* path selection shows an average increased latency of approximately only 4% and a loss rate of 0.5%, whereas a random path selection shows an increased average latency and loss rate of 10% and 2.5%, respectively.

However, there is a limitation on *weighted* multi-path, that is, we assume that the attacker is a passive attacker, and that the user knows which path is being attacked. As a future study, we would like to conduct research on utilizing an optimized path selection algorithm by using the network status of each path and the AS information on the paths to deal with an active attacker who recognizes that the user has changed paths.

4.4. Effectiveness of MMP on Transit-Link DDoS Attack under Large Scale

To measure the effectiveness of MMP under higher latency when using MMP probably increases additional latency by selecting the appropriate paths, we used a larger topology shown in Figure 4 with 6 countries and 18 SCION ASes participating in it. We then used the Google Cloud Platform Computing Engine (GCE) virtual machine as a test client. The following routes $R_{src-dst}$ using the pair of core ASes are used for an evaluation:

- R_{k-s} = {Korea client – Korea core – Switzerland core – Switzerland client},
- R_{k-u} = {Korea client – Korea core – US core – US client},
- R_{k-g} = {Korea client – Korea core – Germany core – Germany client},
- R_{s-u} = {Switzerland client – Switzerland core – US core – US client},
- R_{s-g} = {Switzerland client – Switzerland core – Germany core – Germany client},
- R_{u-g} = {US client – US core – Germany core – Germany client}.

We measured the loss rate of an FMP path and three MMP paths for each $R_{src-dst}$ described above. After the $R_{src-dst}$ is selected, 30,000 SCMP packets with an interval of 0.001 s were sent from one client to another. The test was completed with six $R_{src-dst}$.

Table 3 shows a summary of the test results. From each route $R_{src-dst}$, the FMP path p_0 passes the transit-link directly connected between the selected core source and destination ASes, and MMP paths p_1, p_2, and p_3 are alternative paths not passing the transit-link. The numbers in each table show the loss rates of FMP/MMP paths p_{0-3} under a transit-link DDoS attack. From all routes $R_{src-dst}$, FMP path p_0 that passes the transit-link is affected by 14–32% (average of 19%) significantly by a transit-link DDoS attack, but the other alternative MMP paths show no difference under a DDoS attack and operates properly with MMP routing. Figure 9 shows the average loss rate under bandwidth-based attack. The loss rate of FMP is dramatically increased by the traffic congestion and has 42% when the attack bandwidth is 700 Mbps. However, MMP is stable within 1% loss rate and manages the path to mitigate the congestion.

Table 3. Average loss rate during transit-link DDoS attack. FMP p_0 for each route $R_{src-dst}$ is an FMP path communicating through the transit-link between source and destination. MMP p_1, p_2, and p_3 are alternative paths not passing the transit-link.

Path	R_{k-s}	R_{k-u}	R_{k-g}	R_{s-u}	R_{s-g}	R_{u-g}
FMP: p_0	16%	14%	16%	32%	19%	17%
MMP: p_1	1%	1%	0%	0%	0%	1%
MMP: p_2	1%	1%	1%	0%	0%	1%
MMP: p_3	0%	1%	1%	0%	0%	1%

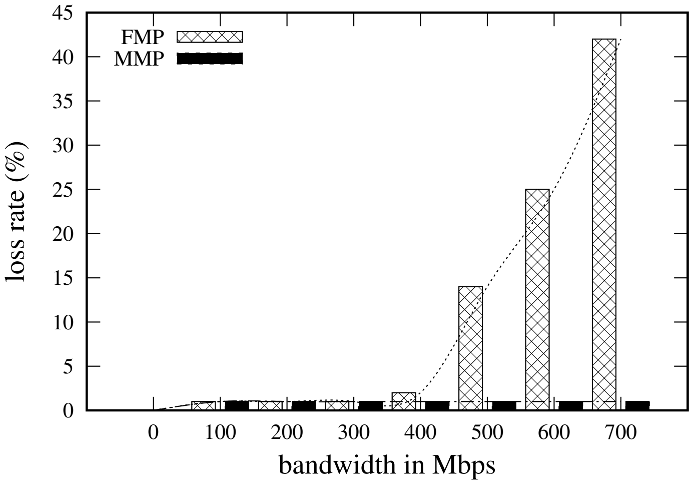

Figure 9. Effect of traffic on FMP. The loss rate is dramatically increased by the traffic congestion on FMP, but MMP manages the path to mitigate the congestion.

5. Research Limitations and Future Work

We measured the latency and the loss rate of SP, FMP, and MMP on a global network using SCION. The results show that MMP routing has a low latency and loss rate compared to FMP routing and more MMP paths show lower latency and loss late. Under the traffic congestion, the loss rate of MMP is stable. However, we can think about the limitation of the operation. If all users of the global network use all possible multi-paths, we could not guarantee the performance of MMP as shown above.

Our suggested future work is to optimize the important factor of MMP operations, such as how many multi-path uses or how many hops of multi-path is the minimum quality for MMP routing. QoS-driven routing is also a possible option for MMP routing policy using QoS metrics, such as latency, loss late, bandwidth, jitter, or other composite metrics. We could make the weight of each multi-path, and some paths could show high latency but stability to communicate.

6. Conclusions

We evaluated multi-path routing on MMP and compared MMP with SP and FMP on a global network. The experimental results show that when using MMP routing, the network performance is affected less by a bandwidth consumption attack than when using SP or FMP routing. In addition, when making a choice among paths under a multi-path situation, selecting more paths with a better network status than paths under an attack causes less effect on the performance of the network under attack.

We verified that the effectiveness of multi-path with real networks deployed globally, especially MMP routing, shows more resilience than FMP used currently. Using the global network, we show that FMP mitigates certain cases of network problems, but MMP gains impressively lower loss rate by comparison.

Author Contributions: Conceptualization, H.A., Y.N., and H.L.; methodology, H.A. and Y.N.; software, Y.N. and A.P.; validation, H.A., H.L., and A.P.; formal analysis, H.A. and H.L.; investigation, H.A.; resources, H.A., Y.N., H.L., and A.P.; data curation, Y.N.; writing—original draft preparation, H.A. and Y.N.; writing—review and editing, H.A., H.L., and A.P.; visualization, H.A. and Y.N.; supervision, H.A. and H.L.; project administration, H.L.; funding acquisition, H.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported in part by the Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2019-0-01343 Regional strategic Industry convergence security core talent training business, No.2019-0-01697 Development of automated vulnerability discovery technologies for blockchain platform security, and No.IITP-2021-2020-0-01819 ICT creative consilience program).

Conflicts of Interest: The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. An, H.; Lee, H.; Perrig, A. Coordination of anti-spoofing mechanisms in partial deployments. *J. Commun. Netw.* **2016**, *18*, 948–961. [CrossRef]
2. Barrera, D.; Chuat, L.; Perrig, A.; Reischuk, R.M.; Szalachowski, P. The SCION internet architecture. *Commun. ACM* **2017**, *60*, 56–65. [CrossRef]
3. Sun, Y.; Edmundson, A.; Vanbever, L.; Li, O.; Rexford, J.; Chiang, M.; Mittal, P. RAPTOR: Routing Attacks on Privacy in Tor. In Proceedings of the 24th USENIX Security Symposium USENIX Security 15, Washington, DC, USA, 12–14 August 2015; pp. 271–286.
4. Labovitz, C.; Ahuja, A.; Bose, A.; Jahanian, F. Delayed Internet routing convergence. *IEEE/ACM Trans. Netw.* **2001**, *9*, 293–306. [CrossRef]
5. Dahlin, M.; Chandra, B.B.V.; Gao, L.; Nayate, A. End-to-end WAN service availability. *IEEE/ACM Trans. Netw.* **2003**, *11*, 300–313. [CrossRef]
6. Paxson, V. End-to-end routing behavior in the Internet. *IEEE/ACM Trans. Netw.* **1997**, *5*, 601–615. [CrossRef]
7. Paxson, V. End-to-end internet packet dynamics. *IEEE/ACM Trans. Netw.* **1999**, *7*, 277–292. [CrossRef]

8. Rekhter, Y.; Li, T. RFC1771: A Border Gateway Protocol 4 (BGP-4). 1995. Available online: https://datatracker.ietf.org/doc/html/rfc1771 (accessed on 18 May 2021).
9. Medhi, D.; Ramasamy, K. *Network Routing: Algorithms, Protocols, and Architectures*; Morgan Kaufmann: Burlington, NC, Canada, 2017.
10. Andersen, D.; Balakrishnan, H.; Kaashoek, F.; Morris, R. Resilient overlay networks. In Proceedings of the Eighteenth ACM Symposium on Operating Systems Principles, Banff, AB, Canada, 21–24 October 2001; pp. 131–145.
11. Raiciu, C.; Paasch, C.; Barre, S.; Ford, A.; Honda, M.; Duchene, F.; Bonaventure, O.; Handley, M. How Hard Can It Be? Designing and Implementing a Deployable Multipath TCP. In Proceedings of the 9th USENIX Symposium on Networked Systems Design and Implementation, San Jose, CA, USA, 25–27 April 2012; pp. 399–412.
12. Jansen, R.; Vaidya, T.; Sherr, M. Point Break: A Study of Bandwidth Denial-of-Service Attacks against Tor. In Proceedings of the 28th USENIX Security Symposium, Santa Clara, CA, USA, 14–16 August 2019.
13. Perrig, A.; Szalachowski, P.; Reischuk, R.M.; Chuat, L. *SCION: A Secure Internet Architecture*; Springer: Berlin/Heidelberg, Germany, 2017.
14. SCION Internet Architecture. Available online: https://www.scion-architecture.net/ (accessed on 18 May 2021).
15. SCIONLab. Available online: https://www.scionlab.org/ (accessed on 18 May 2021).
16. Kwon, J.; Lee, T.; Hähni, C.; Perrig, A. SVLAN: Secure & scalable network virtualization. In Proceedings of the 2020 Network and Distributed System Security Symposium (NDSS 2020, San Diego, CA, USA, 23–26 February 2020.
17. Studer, A.; Perrig, A. The coremelt attack. In *European Symposium on Research in Computer Security*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 37–52.
18. Kang, M.S.; Lee, S.B.; Gligor, V.D. The crossfire attack. In Proceedings of the 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 19–22 May 2013; pp. 127–141.
19. Stewart, R.; Ramalho, M.; Xie, Q.; Tuexen, M.; Conrad, P. *Stream Control Transmission Protocol (SCTP) Partial Reliability Extension*; Technical Report; RFC 3758 (Proposed Standard): Virginia Beach, VA, USA, 2004.
20. Chuat, L.; Perrig, A.; Hu, Y.C. Deadline-Aware Multipath Communication: An Optimization Problem. In Proceedings of the 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Denver, CO, USA, 26–29 June 2017; pp. 487–498.
21. Liu, X.; Mohanraj, S.; Pióro, M.; Medhi, D. Multipath routing from a traffic engineering perspective: How beneficial is it? In Proceedings of the 2014 IEEE 22nd International Conference on Network Protocols, Raleigh, NC, USA, 21–24 October 2014; pp. 143–154.
22. Bellovin, S.M.; Ioannidis, J.; Keromytis, A.D.; Stewart, R.R. On the Use of Stream Control Transmission Protocol (SCTP) with IPSec. 2003. Available online: https://datatracker.ietf.org/doc/html/rfc3554 (accessed on 18 May 2021).
23. Tsirigos, A.; Haas, Z.J. Multipath routing in the presence of frequent topological changes. *IEEE Commun. Mag.* **2001**, *39*, 132–138. [CrossRef]
24. Tsirigos, A.; Haas, Z.J. Analysis of multipath routing-Part I: The effect on the packet delivery ratio. *IEEE Trans. Wirel. Commun.* **2004**, *3*, 138–146. [CrossRef]
25. Papadimitratos, P.; Haas, Z.J. Secure data transmission in mobile ad hoc networks. In Proceedings of the 2nd ACM Workshop on Wireless Security, San Diego, CA, USA, 19 September 2003; pp. 41–50.
26. Pu, C. Jamming-resilient multipath routing protocol for flying ad hoc networks. *IEEE Access* **2018**, *6*, 68472–68486. [CrossRef]
27. Gelenbe, E.; Lent, R.; Nunez, A. Self-aware networks and QoS. *Proc. IEEE* **2004**, *92*, 1478–1489. [CrossRef]
28. Gelenbe, E.; Loukas, G. A self-aware approach to denial of service defence. *Comput. Netw.* **2007**, *51*, 1299–1314. [CrossRef]
29. Sakellari, G.; Gelenbe, E. Demonstrating cognitive packet network resilience to worm attacks. In Proceedings of the 17th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 4–8 October 2010; pp. 636–638.
30. Czachórski, T.; Gelenbe, E.; Kuaban, G.S.; Marek, D. Time-Dependent Performance of a Multi-Hop Software Defined Network. *Appl. Sci.* **2021**, *11*, 2469. [CrossRef]
31. Baldini, G.; Fröhlich, P.; Gelenbe, E.; Hernandez-Ramos, J.L.; Nowak, M.; Nowak, S.; Papadopoulos, S.; Drosou, A.; Tzovaras, D. IoT Network Risk Assessment and Mitigation: The SerIoT Approach. *Secur. Risk Manag.* **2020**, *88*. [CrossRef]
32. Gelenbe, E.; Domanska, J.; Fröhlich, P.; Nowak, M.P.; Nowak, S. Self-aware networks that optimize security, QoS, and energy. *Proc. IEEE* **2020**, *108*, 1150–1167. [CrossRef]
33. Fröhlich, P.; Gelenbe, E.; Nowak, M.P. Smart SDN management of fog services. In Proceedings of the 2020 Global Internet of Things Summit (GIoTS), Dublin, Ireland, 3 June 2020; pp. 1–6.
34. Gelenbe, E. Steps toward self-aware networks. *Commun. ACM* **2009**, *52*, 66–75. [CrossRef]
35. Michel, O.; Keller, E. SDN in wide-area networks: A survey. In Proceedings of the 2017 Fourth International Conference on Software Defined Systems (SDS), Valencia, Spain, 8–11 May 2017; pp. 37–42.
36. Kwon, J.; Seo, D.; Kwon, M.; Lee, H.; Perrig, A.; Kim, H. An incrementally deployable anti-spoofing mechanism for software-defined networks. *Comput. Commun.* **2015**, *64*, 1–20. [CrossRef]
37. Smith, J.M.; Schuchard, M. Routing around congestion: Defeating DDoS attacks and adverse network conditions via reactive BGP routing. In Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–24 May 2018; pp. 599–617.

38. Katz-Bassett, E.; Scott, C.; Choffnes, D.R.; Cunha, Í.; Valancius, V.; Feamster, N.; Madhyastha, H.V.; Anderson, T.; Krishnamurthy, A. LIFEGUARD: Practical repair of persistent route failures. *ACM SIGCOMM Comput. Commun. Rev.* **2012**, *42*, 395–406. [CrossRef]
39. Ballani, H.; Francis, P.; Zhang, X. A study of prefix hijacking and interception in the Internet. *ACM SIGCOMM Comput. Commun. Rev.* **2007**, *37*, 265–276. [CrossRef]
40. Giuliari, G.; Klenze, T.; Legner, M.; Basin, D.; Perrig, A.; Singla, A. Internet backbones in space. *ACM SIGCOMM Comput. Commun. Rev.* **2020**, *50*, 25–37. [CrossRef]
41. Kushman, N.; Kandula, S.; Katabi, D. Can you hear me now?! it must be BGP. *ACM SIGCOMM Comput. Commun. Rev.* **2007**, *37*, 75–84. [CrossRef]