SCION™

ELEVATING SECURE COMMUNICATION

NEXT-GENERATION DDoS DEFENCE WITH SCION

Prof. Yih-Chun Hu

University of Illinois
USA

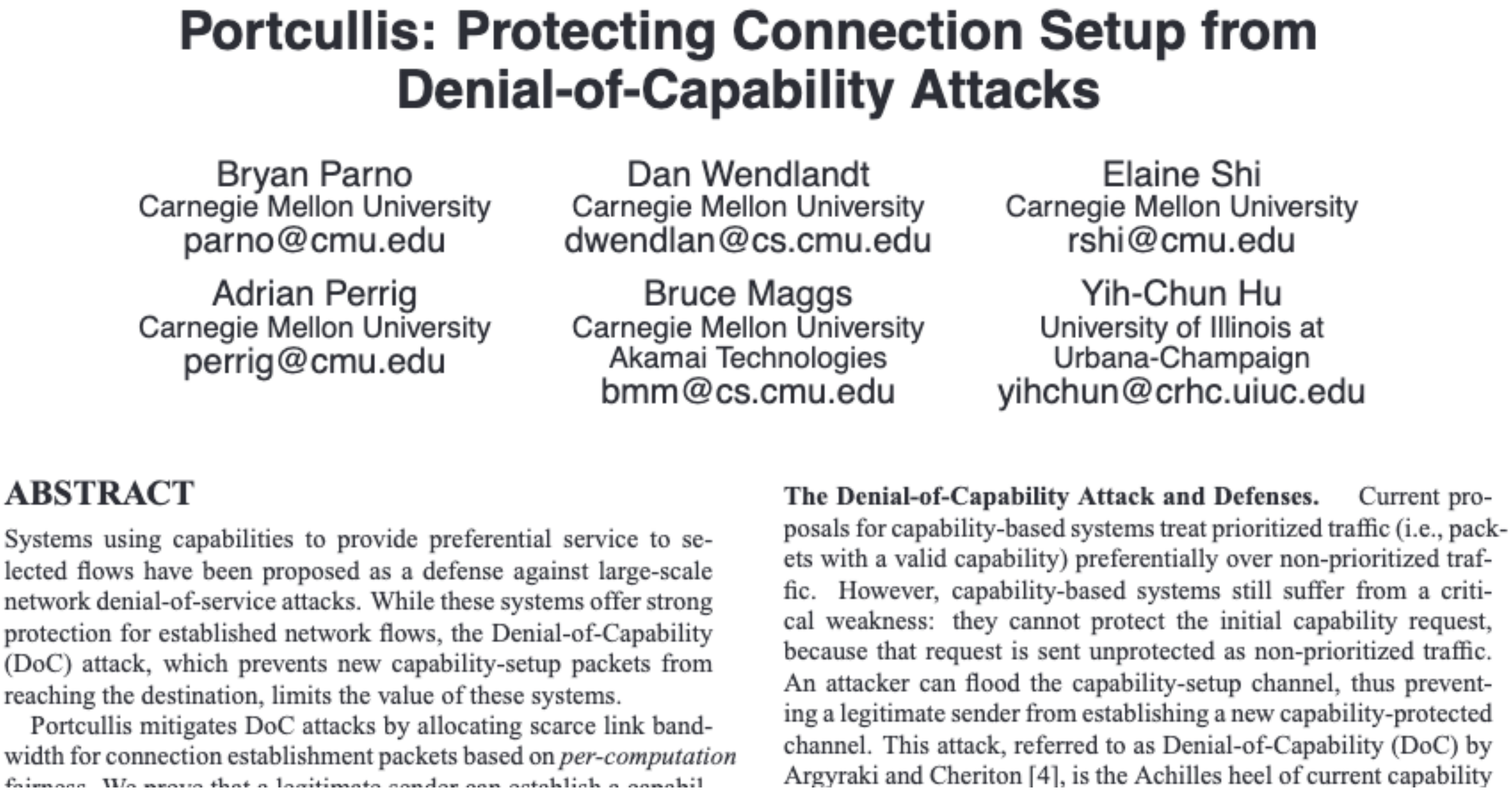
SCION™ ASSOCIATION ETH zürich ANAPAYA eraneos satw technology for society

Next-Generation DDoS Defense with SCION

Yih-Chun Hu
University of Illinois at Urbana-Champaign

October 18, 2023

16 Years Ago



Portcullis: Protecting Connection Setup from Denial-of-Capability Attacks

Bryan Parno
Carnegie Mellon University
parno@cmu.edu

Dan Wendlandt
Carnegie Mellon University
dwendlan@cs.cmu.edu

Elaine Shi
Carnegie Mellon University
rshi@cmu.edu

Adrian Perrig
Carnegie Mellon University
perrig@cmu.edu

Bruce Maggs
Carnegie Mellon University
Akamai Technologies
bmm@cs.cmu.edu

Yih-Chun Hu
University of Illinois at
Urbana-Champaign
yihchun@crhc.uiuc.edu

ABSTRACT

Systems using capabilities to provide preferential service to selected flows have been proposed as a defense against large-scale network denial-of-service attacks. While these systems offer strong protection for established network flows, the Denial-of-Capability (DoC) attack, which prevents new capability-setup packets from reaching the destination, limits the value of these systems.

Portcullis mitigates DoC attacks by allocating scarce link bandwidth for connection establishment packets based on *per-computation fairness*. We prove that a legitimate sender can establish a capabil

The Denial-of-Capability Attack and Defenses. Current proposals for capability-based systems treat prioritized traffic (i.e., packets with a valid capability) preferentially over non-prioritized traffic. However, capability-based systems still suffer from a critical weakness: they cannot protect the initial capability request, because that request is sent unprotected as non-prioritized traffic. An attacker can flood the capability-setup channel, thus preventing a legitimate sender from establishing a new capability-protected channel. This attack, referred to as Denial-of-Capability (DoC) by Argyraki and Cheriton [4], is the Achilles heel of current capability

Why Internet DDoS Defense is Still Hard

No per-packet
source address validation

No roots of trust

No in-network crypto

Inter-AS coordination hard

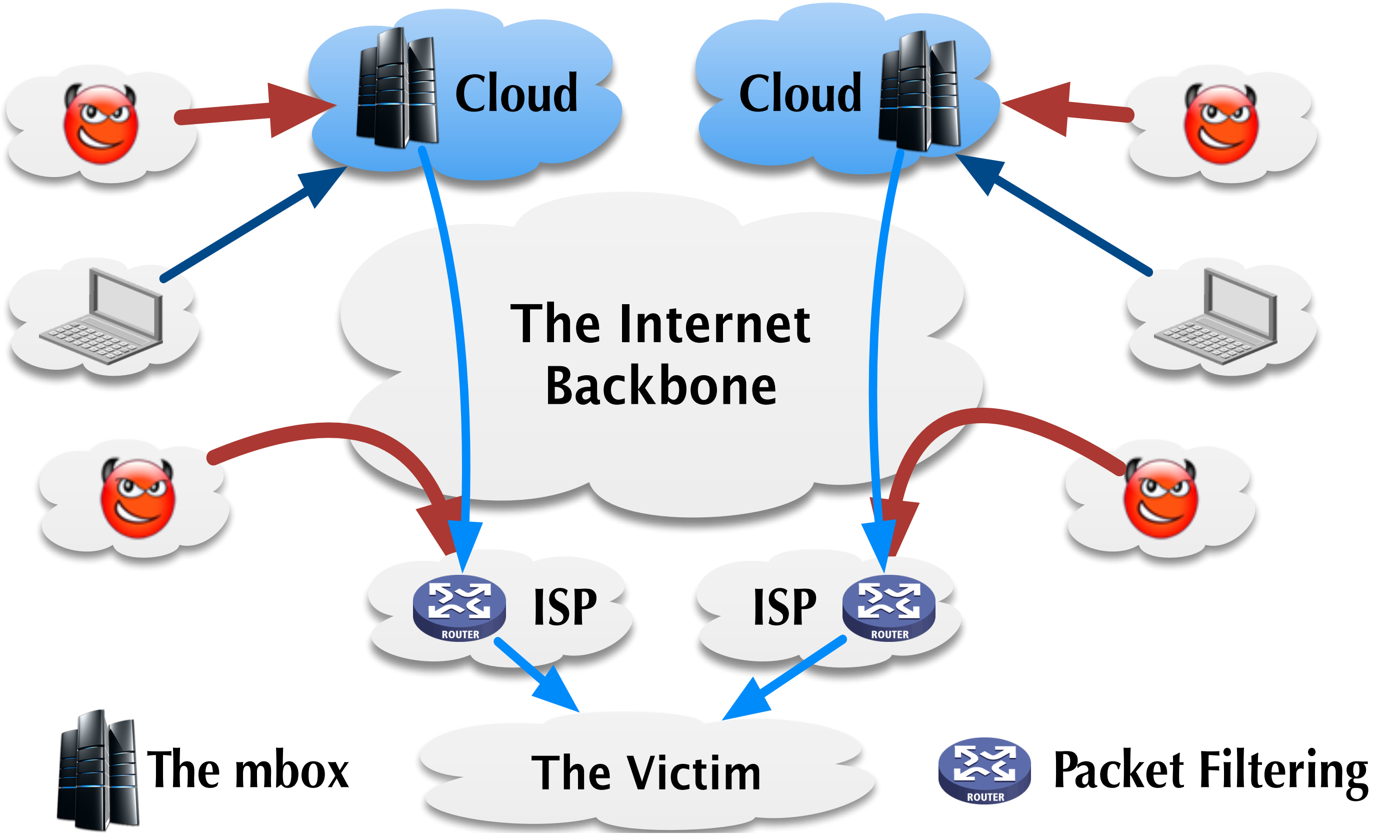
Incremental Deployment

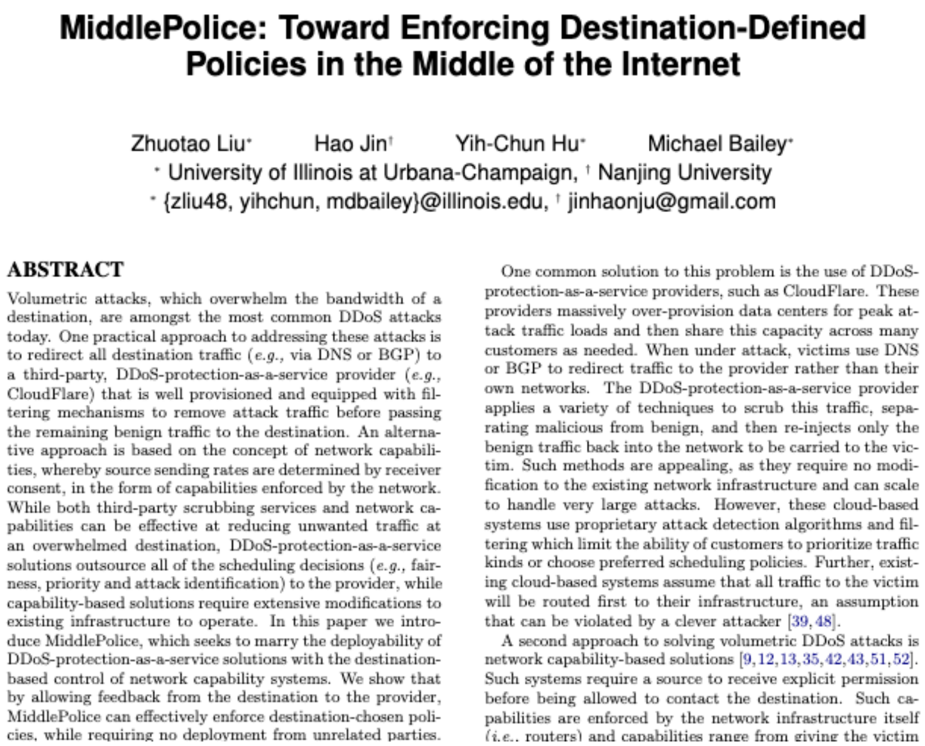
No path transparency

Example Solutions in Today’s Internet

Helping build a better Internet

Example Solutions for Today's Internet





MiddlePolice: Toward Enforcing Destination-Defined Policies in the Middle of the Internet

Zhuotao Liu[*] Hao Jin[†] Yih-Chun Hu[*] Michael Bailey[*]
[*] University of Illinois at Urbana-Champaign, [†] Nanjing University
[*] {zliu48, yihchun, mdbailey}@illinois.edu, [†] jinhaonju@gmail.com

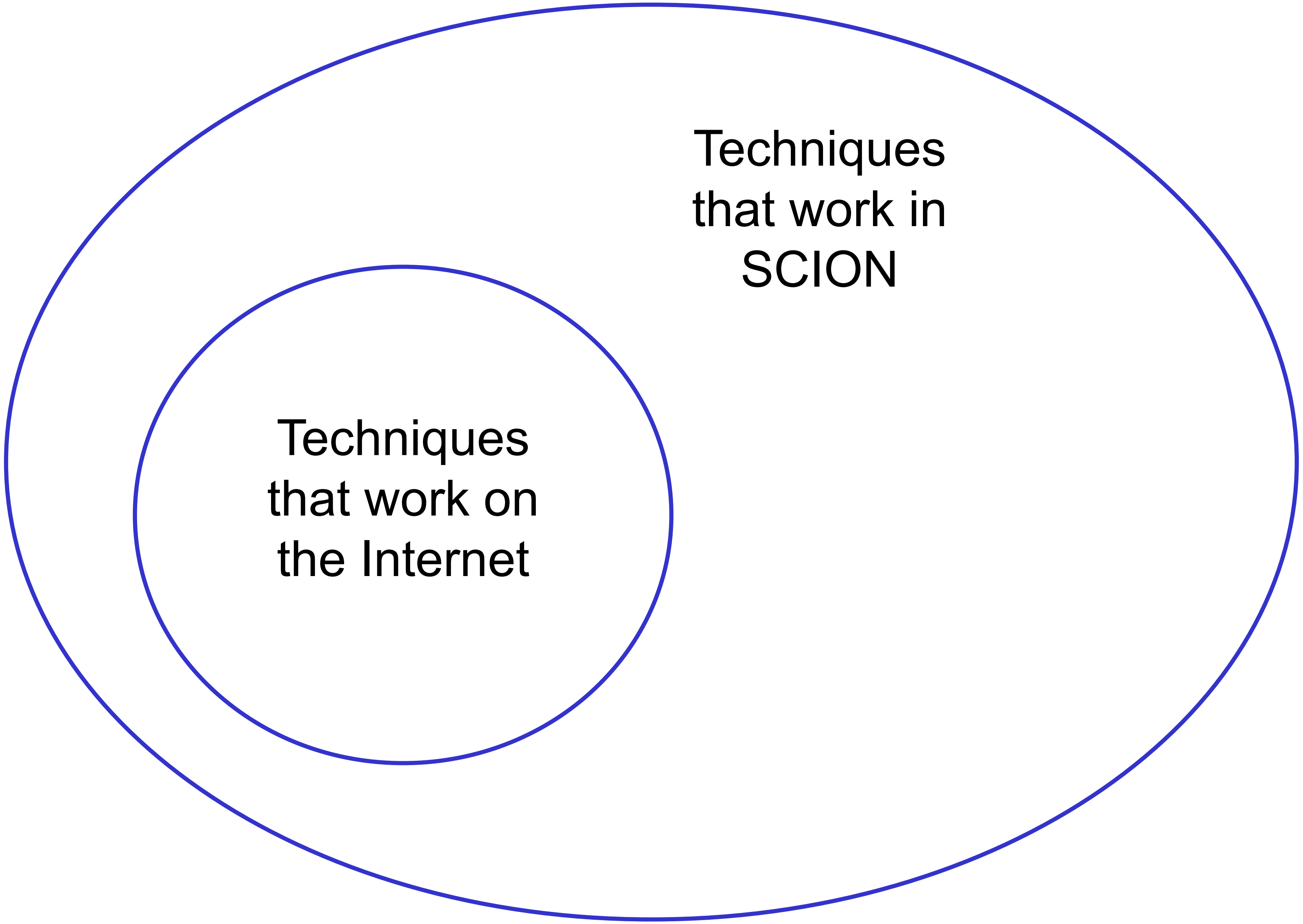
ABSTRACT

Volumetric attacks, which overwhelm the bandwidth of a destination, are amongst the most common DDoS attacks today. One practical approach to addressing these attacks is to redirect all destination traffic (*e.g.*, via DNS or BGP) to a third-party, DDoS-protection-as-a-service provider (*e.g.*, CloudFlare) that is well provisioned and equipped with filtering mechanisms to remove attack traffic before passing the remaining benign traffic to the destination. An alternative approach is based on the concept of network capabilities, whereby source sending rates are determined by receiver consent, in the form of capabilities enforced by the network. While both third-party scrubbing services and network capabilities can be effective at reducing unwanted traffic at an overwhelmed destination, DDoS-protection-as-a-service solutions outsource all of the scheduling decisions (*e.g.*, fairness, priority and attack identification) to the provider, while capability-based solutions require extensive modifications to existing infrastructure to operate. In this paper we introduce MiddlePolice, which seeks to marry the deployability of DDoS-protection-as-a-service solutions with the destination-based control of network capability systems. We show that by allowing feedback from the destination to the provider, MiddlePolice can effectively enforce destination-chosen policies, while requiring no deployment from unrelated parties.

One common solution to this problem is the use of DDoS-protection-as-a-service providers, such as CloudFlare. These providers massively over-provision data centers for peak attack traffic loads and then share this capacity across many customers as needed. When under attack, victims use DNS or BGP to redirect traffic to the provider rather than their own networks. The DDoS-protection-as-a-service provider applies a variety of techniques to scrub this traffic, separating malicious from benign, and then re-injects only the benign traffic back into the network to be carried to the victim. Such methods are appealing, as they require no modification to the existing network infrastructure and can scale to handle very large attacks. However, these cloud-based systems use proprietary attack detection algorithms and filtering which limit the ability of customers to prioritize traffic kinds or choose preferred scheduling policies. Further, existing cloud-based systems assume that all traffic to the victim will be routed first to their infrastructure, an assumption that can be violated by a clever attacker [39, 48].

A second approach to solving volumetric DDoS attacks is network capability-based solutions [9,12,13,35,42,43,51,52]. Such systems require a source to receive explicit permission before being allowed to contact the destination. Such capabilities are enforced by the network infrastructure itself (*i.e.*, routers) and capabilities range from giving the victim

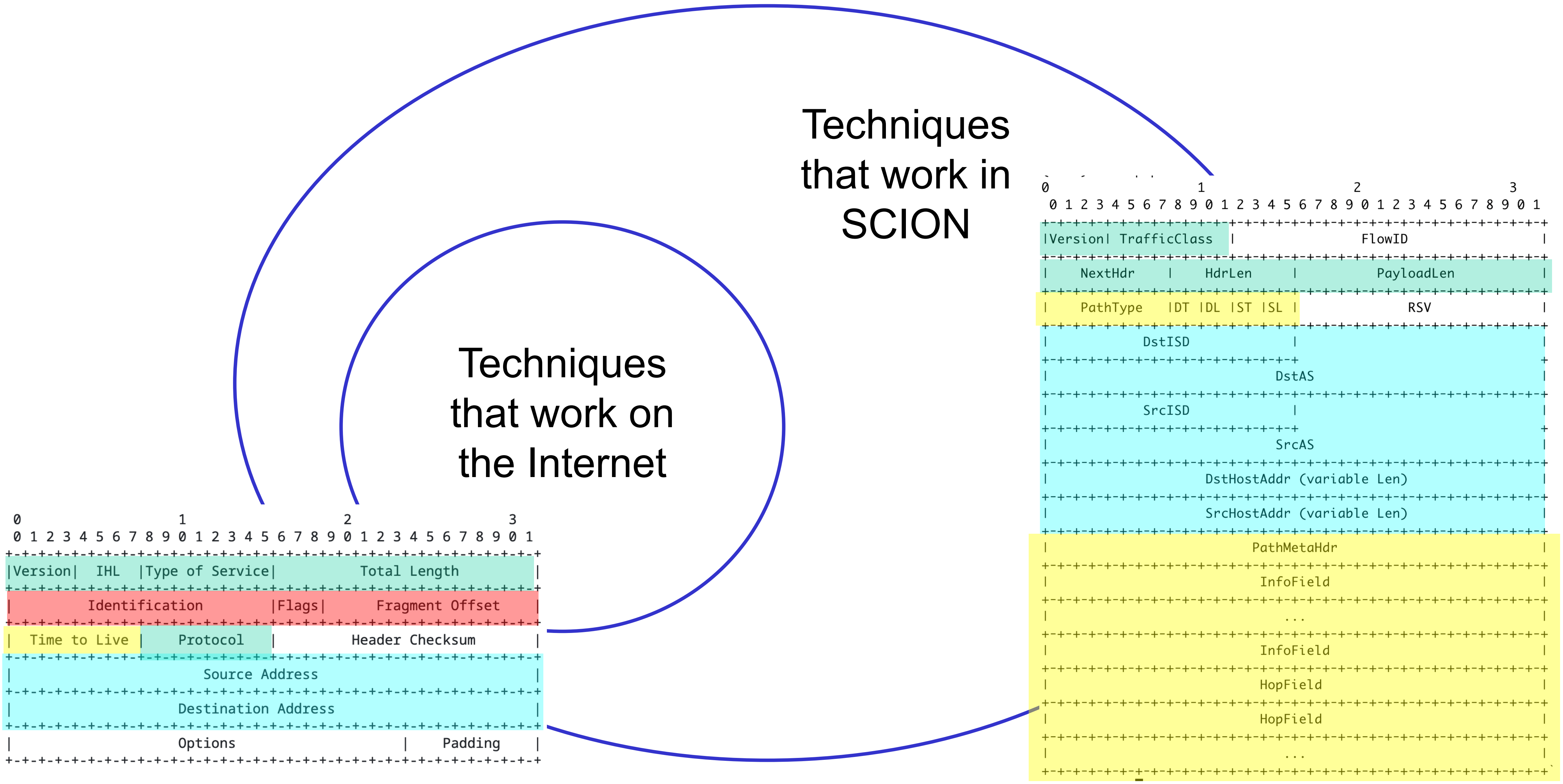
Works on the Internet ⇒ Works in SCION



Techniques that work in SCION

Techniques that work on the Internet

Works on the Internet ⇒ Works in SCION



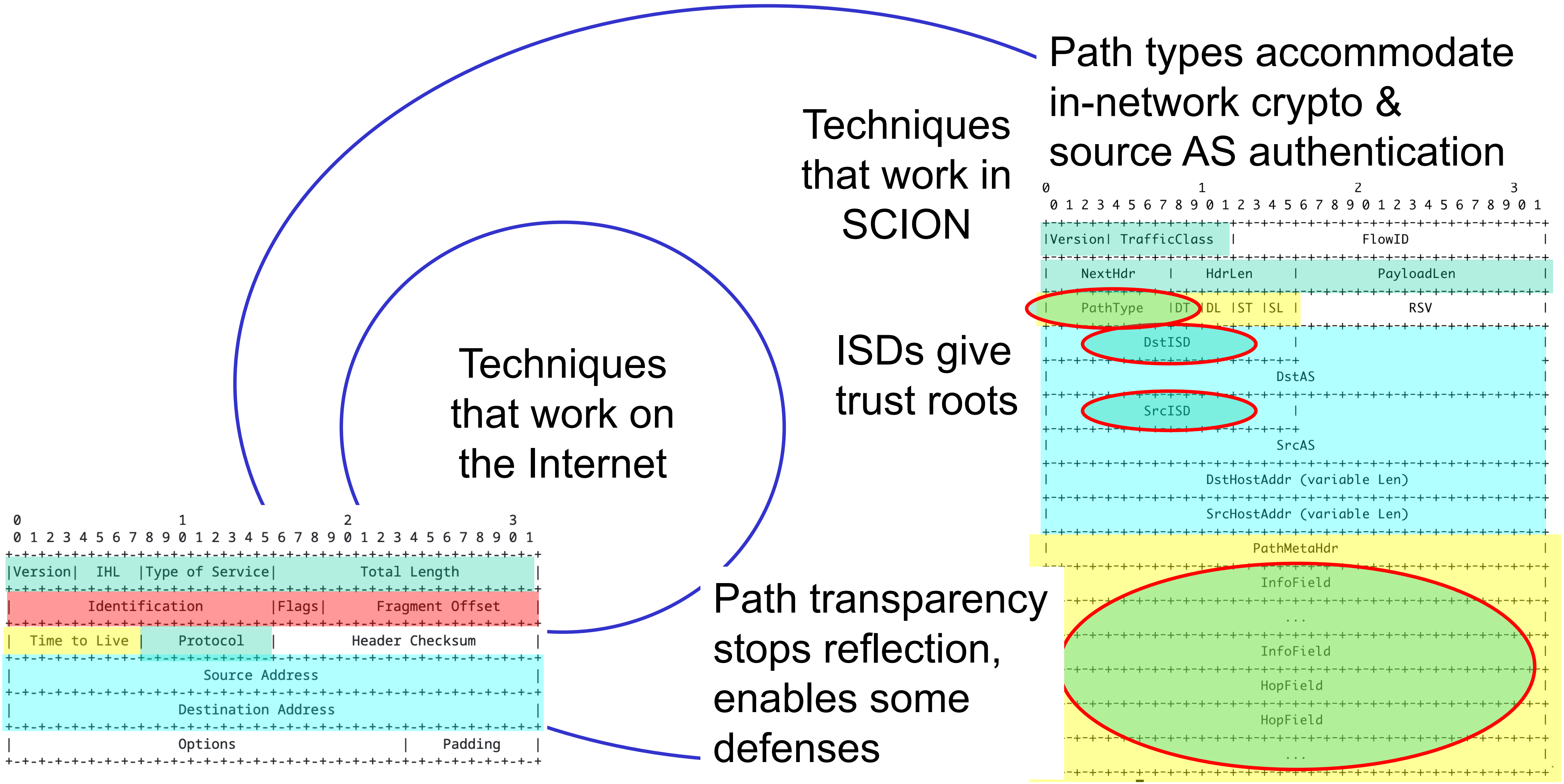
Techniques that work in SCION

Techniques that work on the Internet

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| TrafficClass  |                FlowID                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    NextHdr    |    HdrLen     |          PayloadLen           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    PathType   |DT |DL |ST |SL |              RSV              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            DstISD             |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               +
|                             DstAS                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            SrcISD             |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               +
|                             SrcAS                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    DstHostAddr (variable Len)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    SrcHostAddr (variable Len)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          PathMetaHdr                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           InfoField                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              ...                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           InfoField                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           HopField                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           HopField                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              ...                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Works on the Internet ⇒ Works in SCION



Techniques that work in SCION

Techniques that work on the Internet

Path types accommodate in-network crypto & source AS authentication

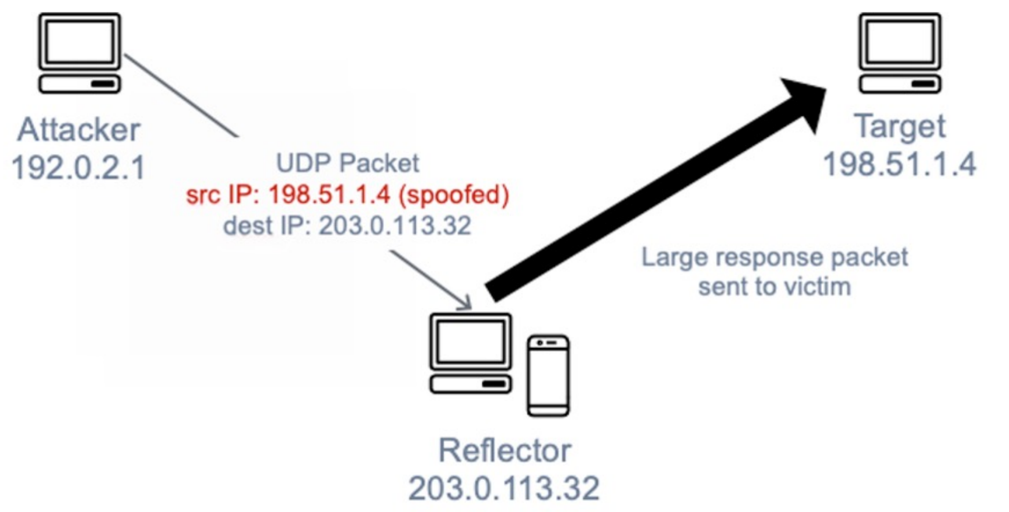
ISDs give trust roots

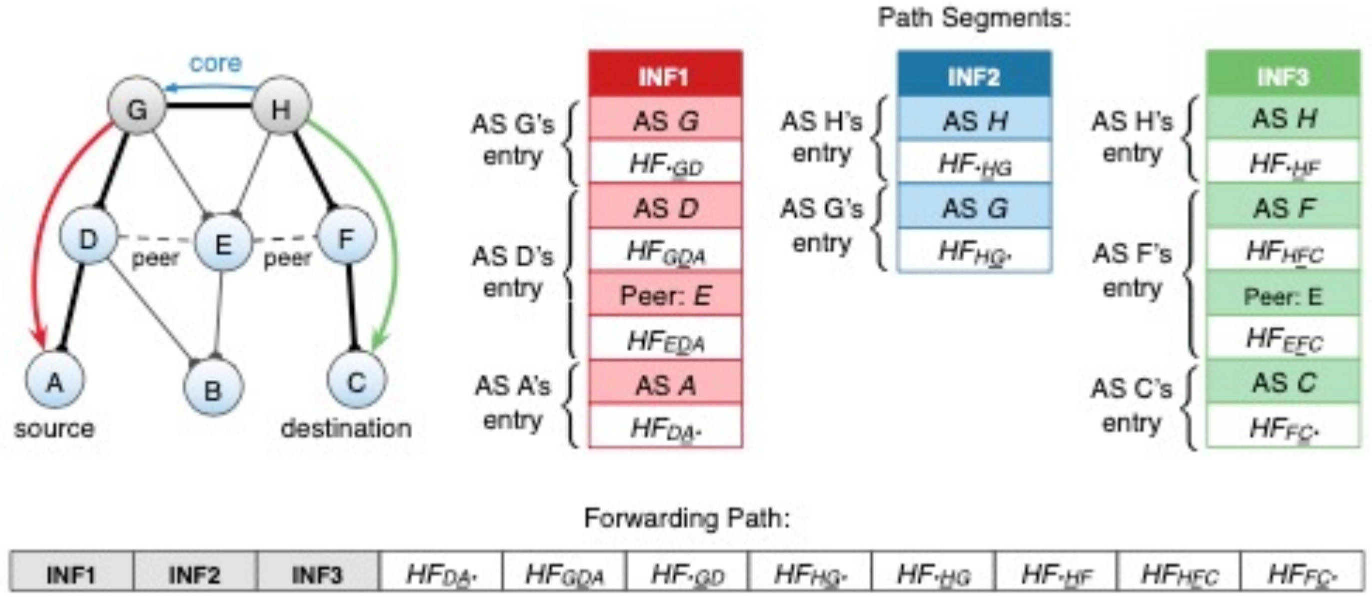
Path transparency stops reflection, enables some defenses

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| TrafficClass  |                FlowID                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    NextHdr    |    HdrLen     |          PayloadLen           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    PathType   |DT |DL |ST |SL |              RSV              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            DstISD             |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               +
|                             DstAS                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            SrcISD             |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               +
|                             SrcAS                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    DstHostAddr (variable Len)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    SrcHostAddr (variable Len)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          PathMetaHdr                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           InfoField                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              ...                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           InfoField                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           HopField                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           HopField                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              ...                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Stopping Reflection: Path Reversal





Path Segments:

	INF1
AS G's entry	AS *G*
	$HF_{\cdot \underline{G}D}$
AS D's entry	AS *D*
	$HF_{G\underline{D}A}$
	Peer: *E*
	$HF_{E\underline{D}A}$
AS A's entry	AS *A*
	$HF_{D\underline{A}\cdot}$

	INF2
AS H's entry	AS *H*
	$HF_{\cdot \underline{H}G}$
AS G's entry	AS *G*
	$HF_{H\underline{G}\cdot}$

	INF3
AS H's entry	AS *H*
	$HF_{\cdot \underline{H}F}$
AS F's entry	AS *F*
	$HF_{H\underline{F}C}$
	Peer: E
	$HF_{E\underline{F}C}$
AS C's entry	AS *C*
	$HF_{F\underline{C}\cdot}$

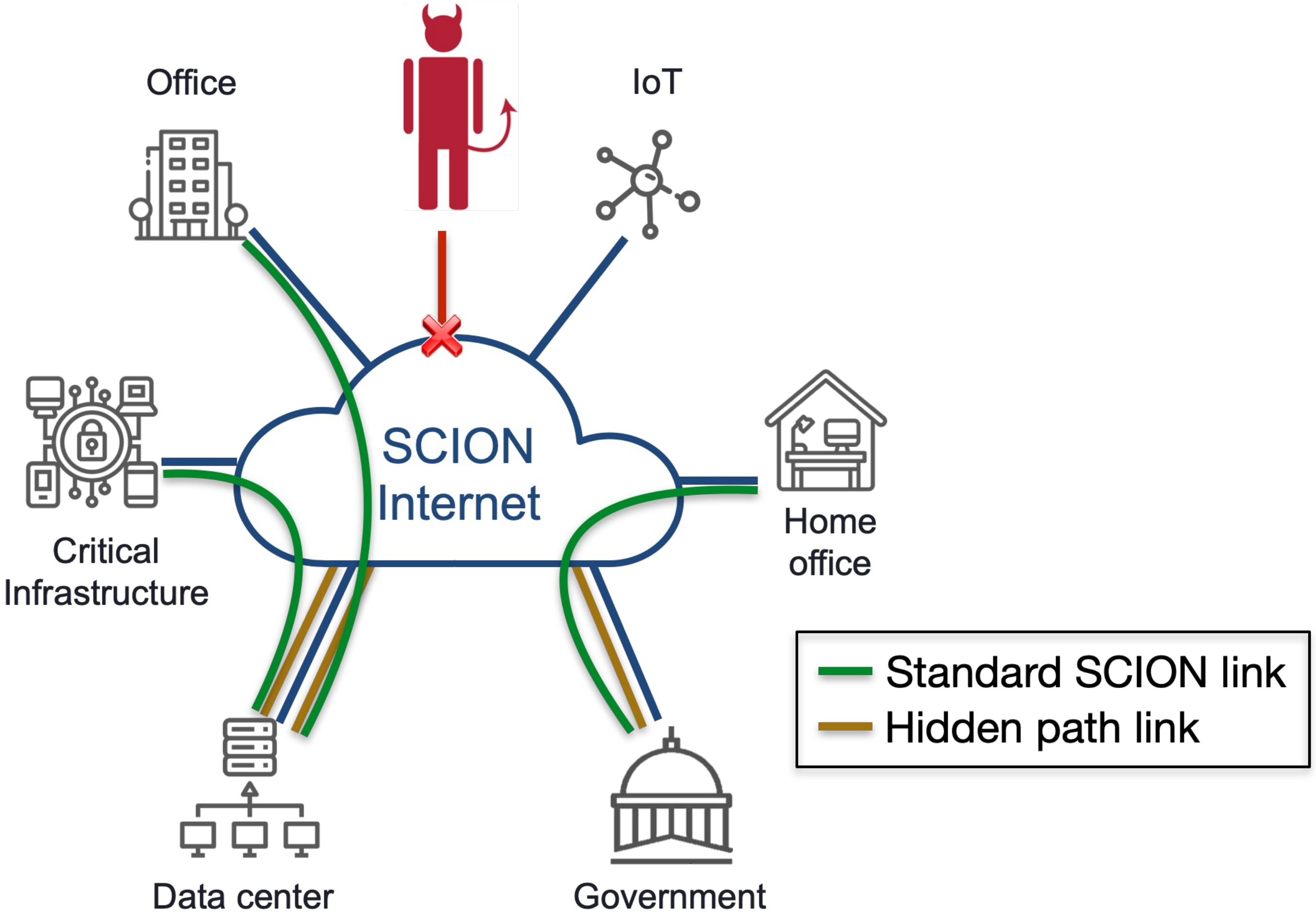
Forwarding Path:

INF1	INF2	INF3	$HF_{D\underline{A}\cdot}$	$HF_{G\underline{D}A}$	$HF_{\cdot \underline{G}D}$	$HF_{H\underline{G}\cdot}$	$HF_{\cdot \underline{H}G}$	$HF_{\cdot \underline{H}F}$	$HF_{H\underline{F}C}$	$HF_{F\underline{C}\cdot}$

Figure 5.9: An example of a path traversing core ASes.

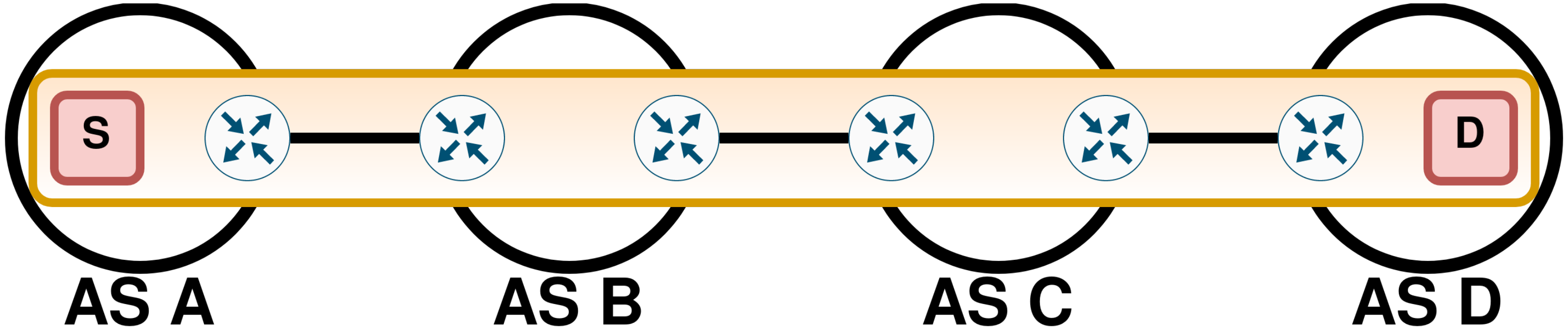
Avoiding DDoS Traffic with Path Migration

- Path migration
  - Built on SCION's path dissemination and path validators



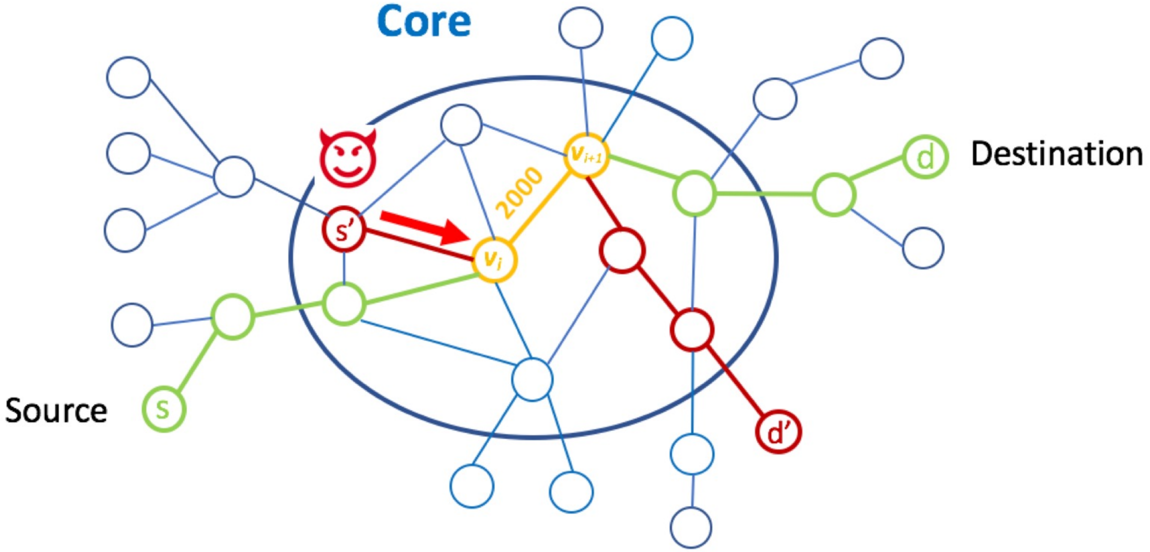
SCION Features Enable Reservations

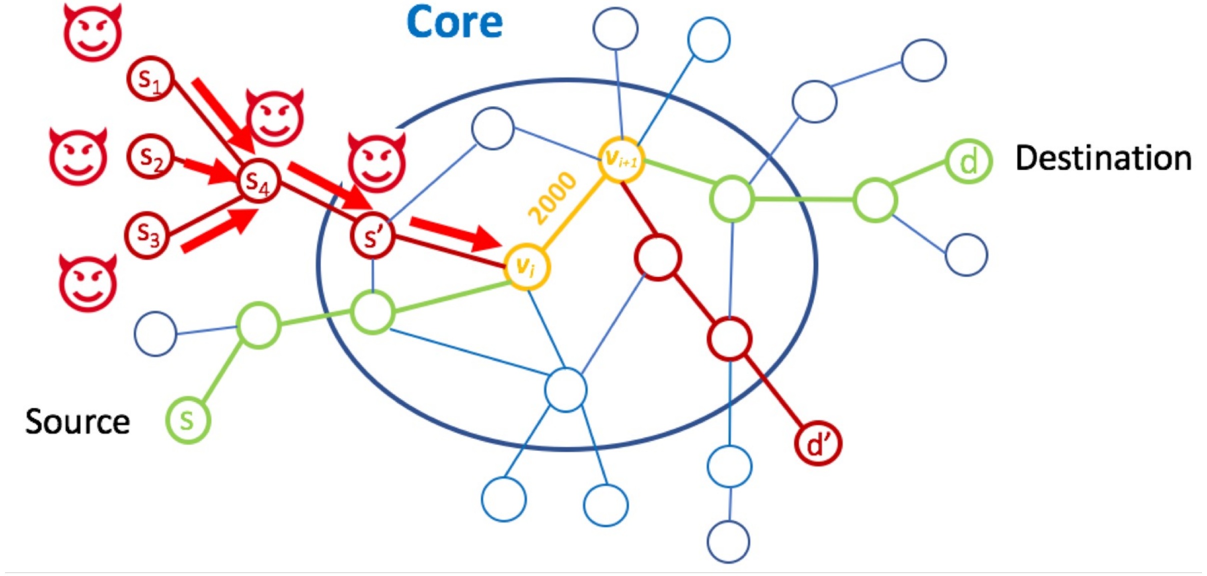
- Trust roots
  - Established by ISDs, removes need for global root of trust
- Per-packet, per-hop Source Authentication (EPIC or SPAO)
  - Built on DRKey, allows first packet to be authenticated
- In-network reservations with guaranteed bandwidth (COLIBRI)
  - Built on source AS authentication, duplicate suppression, large flow detection
- Provides fairness guarantees even against Crossfire-style attacks



Who Gets Reservations?

- Two Approaches to DDoS:
  - Identify the attackers, remove their traffic
  - Some fairness notion
- SCION tools for source AS and user identity allow network to enforce many different fairness notions
  - e.g., COLIBRI per-source-AS fairness

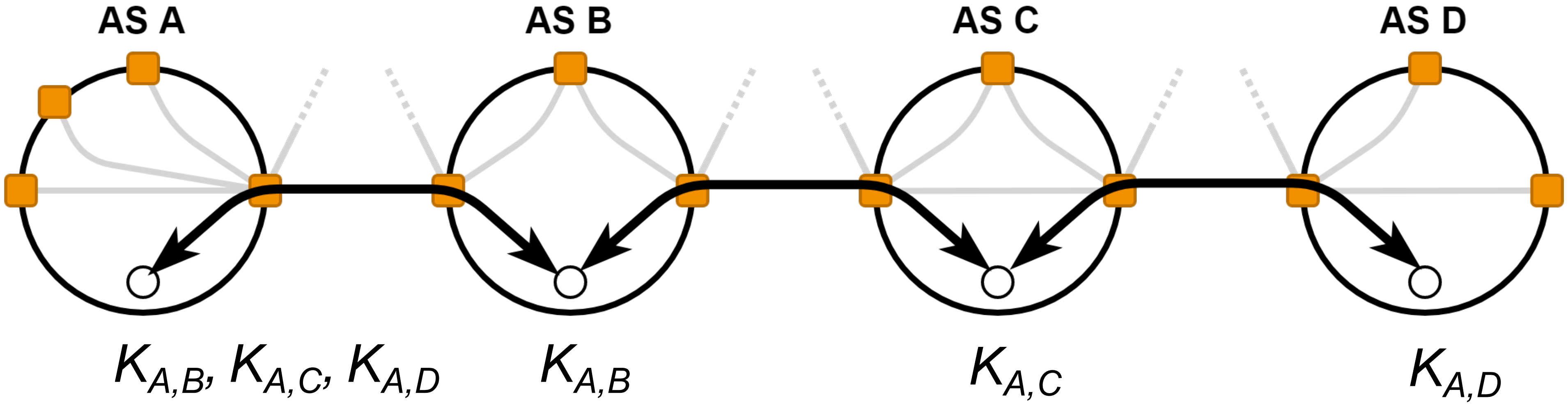




SCION Features Enable In-Network Fairness Notions

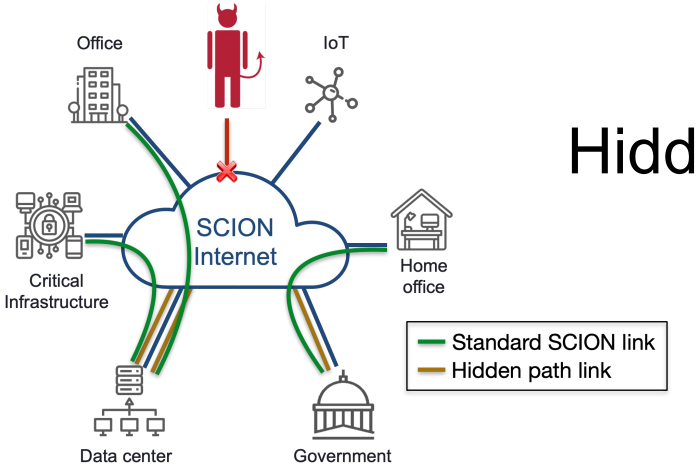
- Per-packet, per-hop Source Authentication (EPIC or SPAO)
  - Built on DRKey, allows first packet to be authenticated

- Allows for in-network per-packet enforcement of arbitrary fairness notions
  - e.g., LightningFilter
  - e.g., GMA and DoCile

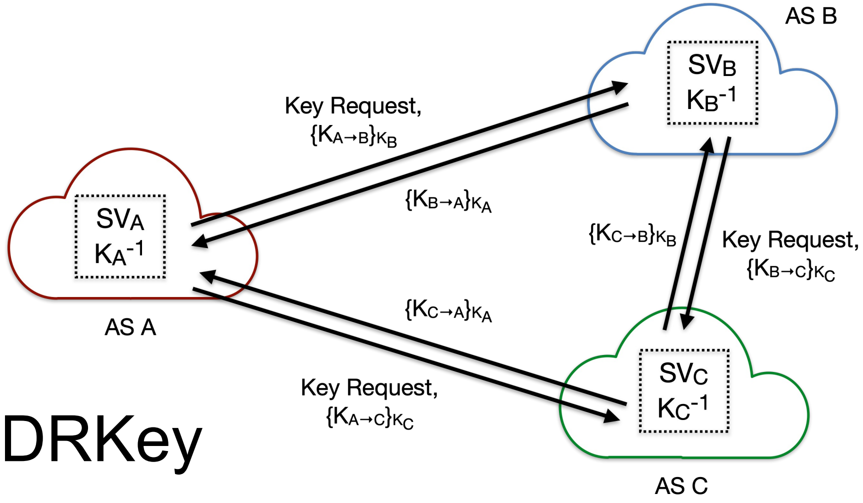


In Today’s SCION

- Hidden paths available in production SCION
- DRKey, COLIBRI and EPIC available in SCIONLab

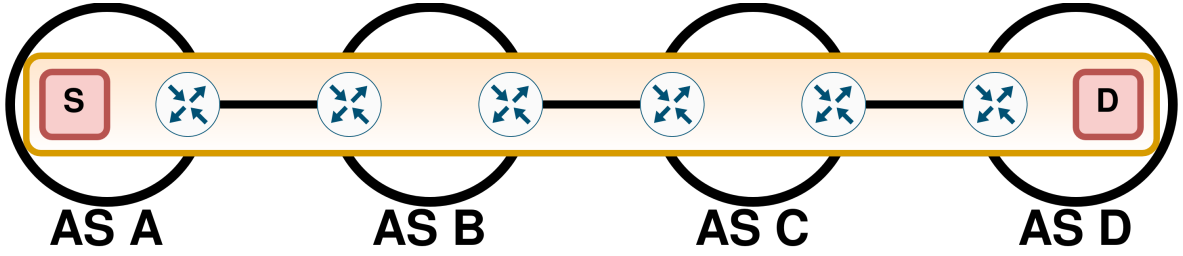


Hidden Paths



DRKey

COLIBRI



EPIC Level 2

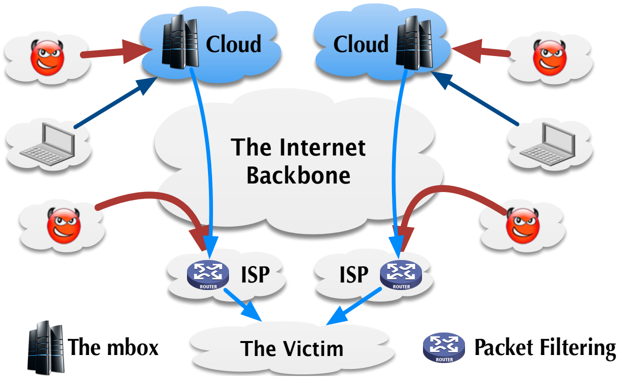
- Goal: **line-speed source authentication for every packet on every router**
- Approach: include DRKey $K_{X\to Y:H}$ in hop field MAC
- $K_H = MAC_{K_i}($ TS || IgIF || EgIF || ExpT || S_{i-1})
  $S_i = H(K_H)$
  Hop field MAC: $MAC_{K_{X\to E:e}}(T \| H(P) \| len(P) \| K_H)$
  For host e in AS E, traversing AS X
- Router in AS X can efficiently derive $K_{X\to E:e}$ (2 AES operations)
- Host e needs to fetch one key per AS traversed from local certificate server
- Result: efficient per-packet per-hop source authentication!
  (5 AES op)

Conclusions

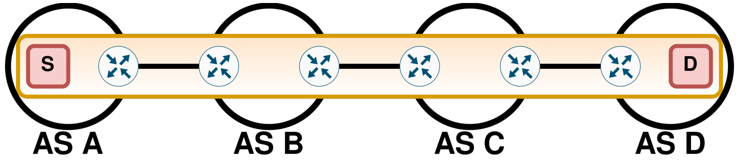
- Anything that works on the Internet works in SCION

CLOUDFLARE®

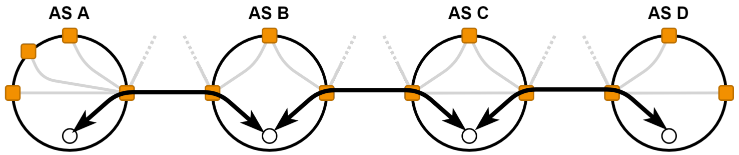
Helping build a better Internet



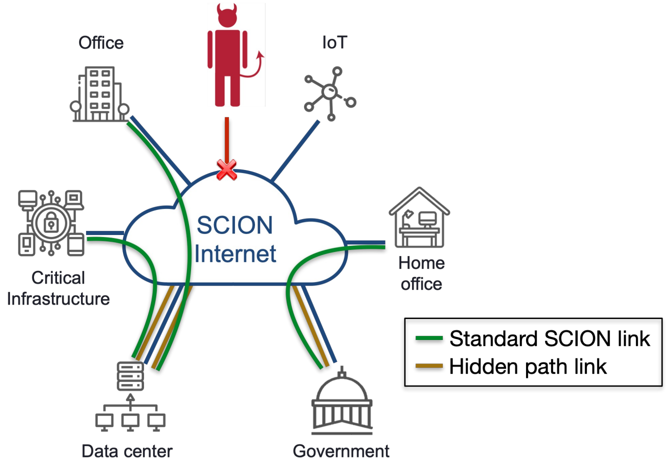
- SCION has a suite of protocols, built on uniquely-SCION features, that defend against DDoS, but cannot be used on the Internet



COLIBRI



DoCile



Path Migration