Source Packet Routing in Networking (SPRING)

Adrian Reuter
Betreuer: M.Sc. Edwin Cordeiro
Seminar Future Internet WS2016
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: adrian.reuter@tum.de

ABSTRACT
This paper analyses the source routing strategy, which is an alternative to the shortest-path-first strategy. It depicts use cases for source routing and provides an insight into a new source routing mechanism currently developed by the IETF SPRING working group. The design requirements identified by the working group as well as the proposed architecture and implementational approaches are explained. The paper further presents alternative source routing solutions and compares them to the SPRING working group solution. The paper concludes with a prospect of challenges that the SPRING solution is likely to face in deployment.

Keywords
Source Routing, Source Packet Routing, Segment Routing, MPLS, SPRING, RPL, DSR, RH0

1. INTRODUCTION
Within internetworking infrastructure, the shortest path - respective to the metric in use - is the most common standard strategy for forwarding decisions. Routers interconnect separate networks and forward traffic from the source to the destination. Every router decides on its own where to steer a packet, according to its Routing Information Base (RIB) and its Forwarding Information Base (FIB). The information stored in these bases are established either manually or via routing protocols. Interior Gateway Protocols (IGP) such as OSPF or IS-IS are used to exchange routing information between routers within an Autonomous System (AS), whereas Exterior Gateway Protocols (EGP) such as BGP are used to communicate routing information between autonomous systems [1].

However, there are multiple scenarios in which a node may wish to determine a specific set of nodes that shall be traversed while delivering a packet to its destination, or even impose an explicit path through the network topology for reaching the destination. The strategy of imposing a partial or entire path on a packet is called *Source Routing* and can be a powerful mean towards efficient and programmable networks [2]. For this reason this paper will depict the manifold use cases for source routing and present source routing solutions that have been implemented or are currently in development.

Sections 1.1 and 1.2 provide an insight into mechanisms and protocols that are crucial for understanding the work in development by the SPRING working group. While section 2 concentrates on the source routing solution that is currently developed by the IETF, section 3 presents alternative solutions originating from academic research, standardisation organisations or industrial development.

1.1 IPv6 Extension Headers
The Internet Protocol Version 6 (IPv6) is located on the network layer (layer 3) of the ISO/OSI model and offers logical end-to-end addressing for network communication. Besides the standard header fields that most notably include source and destination address, IPv6 provides the ability to attach additional information to IP packets by so-called extension headers. Extension headers enable extended and optional functionalities for IP packets, such as fragmentation, routing options, authentication or encrypted encapsulation [3]. They consist of a 'Next Header' field indicating the subsequent header type, a 'Hdr Ext Len' field defining the length of the extension header, and varying header-specific data [4]. Extension headers immediately follow the IPv6 standard header and are announced by the 'Next Header' field of the preceding header. That means the standard header might announce an extension header in its 'Next Header' field, while the extension header announces another extension header (or a layer 4 protocol header) in its own 'Next Header' field [3].

1.2 Multiprotocol Label Switching (MPLS)
Conventional routers make their forwarding decisions according to a longest prefix match. This results in each and every router along the path to the destination deciding on its own where to route a packet; choosing the longest match between the destination IP address of the incoming packet and the network addresses with their prefix lengths stored in the Routing Information Base [1]. Multiprotocol Label Switching (MPLS) is used mostly in backbone networks, service provider networks or huge company networks, and enables routers within a MPLS-domain to forward packets only according to a prepended *label*. Such a label specifies the affiliation of a packet to a *Forwarding Equivalence Class (FEC)*, which is defined by RFC 3031 [5] as *"a group of IP packets which are forwarded in the same manner (e.g., over the same path, with the same forwarding treatment)"*.

A MPLS-enabled router at the border of a MPLS-domain analyzes incoming IP datagrams and assigns them to a FEC by prepending a 20-bit label. As consequence the network layer protocol and its addressing scheme is only analyzed once, that is when entering the MPLS-domain [5]. The la-

doi: 10.2313/NET-2017-05-1_05

bel is most commonly prepended with the help of a so-called *shim header*, a small header inserted between the layer 2 and layer 3 headers [5]. Other MPLS routers within the domain will forward the packet based on the label. They can also add further labels to the packet and thus create a label stack. Label meanings are exchanged between routers by dedicated protocols such as LDP and RSVP, or extensions to other protocols such as BGP [5].

2. SPRING WORKING GROUP

In order to advance the research and standardization of a flexible and universal source routing mechanism, the Internet Engineering Task Force (IETF) has formed a working group (WG) in 2013. This WG, called *Source Packet Routing in Networking (SPRING)*, is chartered to identify source routing use cases as well as defining the requirements and mechanisms for implementing, deploying and administrating source routing enabled networks [6]. The working group yet developed a new source routing mechanism called *segment routing* [7], which is discussed in section 2.3. It further introduced two implementational approaches [8, 9], which will be discussed in section 2.4 and 2.5. The working group is currently preparing their final document revisions for a technical review and adoption to IETF standards track [10].

2.1 Requirements and Design Goals

The SPRING WG charter [6] defines some fundamental design goals and general requirements for the new source routing mechanism to be worked on. With regard to IPv6 replacing IPv4 in near future, the working group agreed on not taking IPv4 into consideration and developing an IPv6-only based solution [6]. The new source routing mechanism is ought to be downward compatible with existing protocols and layers and should minimize modifications to existing architectures. This is a central requirement for an incremental and selective enrollment of the new mechanism in the context of existing network hardware resources and infrastructures [2]. To be able to traverse non-source-routed network sections, the new source routing solution needs to provide interoperability with conventional non-source-routed networks or subnets [6].

Furthermore intermediate routers shall be able to forward packets based on routing information attached to the packets themselves instead of per-path state information stored at those intermediate routers. That means the path (or a partial path) to be taken to reach the destination is encoded in the packet header, and is not decided by routers on the path. It is important to notice that the node imposing the source-routed path (in the following proceeding denoted as 'source') is not necessarily the originator of a packet, but might also be for example a router at the border of a source-routed domain [6]. After all, the SPRING WG solution must define a basic security concept to encounter common security issues, such as malicious packet injection or traffic amplification. This security concept might be enhanced by additional security mechanisms deployed by the operator, individually fitting the needs [2, 6].

2.2 Source Routing Use Cases

Source routing is a useful technique for various reasons. In a nutshell, source routing can be particularly used for tunneling network traffic, offers resiliency enhancing possibilities and allows for simplified traffic engineering. Of course further potential use cases exist and might show up as soon as source routing found wide adoption and a stable and universial standard mechanism has been released.

2.2.1 Traffic Engineering

Xiao et al. provide a concise definition of traffic engineering [11], stating that *"Traffic Engineering is the process of controlling how traffic flows through one's network so as to optimize resource utilization and network performance"*. Additionally to the optimization aspect, traffic engineering also allows for implementing service level agreements from a technical point of view, e.g fulfilling agreements between customer and internet service provider about guaranteed bandwidth, delay, stability or throughput [12]. Besides performance concerns, source routing can help implementing formal requirements or administrative policies for traffic transmission and traffic separation, e.g. governmental dictations or separation of security sensitive traffic flows in certain businesses [12].

It is obvious that traffic engineering is an indispensable measure in todays backbone networks, service provider networks and large enterprise networks that consist of many routers, redundant links and alternative paths to increase reliability, enhance performance and avoid congestion [13]. Using source routing, alternate paths to the same destination can be easily imposed to a packet without the need of stateful per-flow routing information established on intermediate nodes, which would elsewise be needed to decide where to forward a packet [12]. Load sharing and load balancing can be achieved by source routing traffic over different paths, even through non-parallel links and even if two distinct paths share the same costs (Equal Cost Multiple Path (ECMP) routing) [2].

2.2.2 MPLS Tunneling

Source Routing in combination with MPLS is a useful and efficient technique to build *Virtual Private Networks (VPN)*, that are transparent for users. IP-based tunneling mechanisms such as IPsec or L2TP encapsulate IP traffic within IP datagrams and thereby rely on the forwarding mechanism of the IP protocol themselves.

However, MPLS allows to tunnel IP traffic seemlessly without encapsulating it into a network layer protocol again, while providing a more direct access on path selection. Moreover internet service providers sometimes also offer *Virtual Private Wire Services (VPWS)*, meaning they connect spatially distributed customer networks on link layer basis by tunneling link layer traffic via their backbone networks [14]. Source routing, which can be implemented on MPLS data plane [2], enables operators to more efficiently create such tunnels and control the data flows and path selections in a direct manner [12].

2.2.3 Resiliency use cases

Source routing constitutes a base mechanism for increasing resiliency, offering fast rerouting capabilities by allowing imposition of alternative paths [2]. Resiliency can be improved by calculating backup paths through a network topology in order to face link failures or node failures on the designated

doi: 10.2313/NET-2017-05-1_05

path from source to destination [2, 15]. Path protection is a technique that augments resilience by calculating a complete disjoint secondary path from source to destination, i.e. using only disjoint intermediate nodes and links to reach the destination [15].

In contrast to path protection, resiliency can be also improved by either bypassing only a faulty link and then returning to the originally designated path, or by bypassing the entire faulty node and thus using an alternative shortest path to the destination [15]. Furthermore source routing can be a mean to bridge temporary microloops [2], which might occur during the short-lived convergence phase of the IGP protocol in use, as routing information is not consistent across all routers at this point time [15]. Source routing helps avoiding these temporary microloops by imposing an explicit path through the network topology to all packets that need to be forwarded during the convergence phase. The latter is possible because source routing can operate independently and regardless of inconsistent routes, metrics, and priorities that are being established during convergence phase and which are causing these loops [15].

2.3 Segment Routing

Segment routing is a new source routing mechanism developed by the IETF SPRING working group. It is based on so-called *segments* [7]. The SPRING architecture [7] defines that a segment represents *"an instruction a node executes on the incoming packet (e.g.: forward packet according to shortest path to destination, or, forward packet through a specific interface, or, deliver the packet to a given application/service instance)"*. A segment and its associated *Segment Identifier (SID)* is advertised within the segment routing domain with the help of the Interior Gateway Protocol (IGP) in use. Therefore the SPRING working group has defined extensions for the IGP protocols OSPF [16], OSPFv3 [17] and IS-IS [18]. With the help of these extensions, those protocols are able to carry the necessary segment routing signaling information. Segment routing introduces three major types of segments [19, 7]:

- IGP-Prefix Segments
- IGP-Node Segments
- IGP-Adjacency Segments

Each of these segment types are discussed in the following sections. The term *ingress node* identifies the node at which a packet enters the segment routing domain, whereas *egress node* identifies the node at which a packet exits the segment routing domain.

2.3.1 IGP-Node Segment

An IGP-node segment has global scope and thus is identified by a globally unique SID. Each node is assigned a SID and advertises its nodal segment via the IGP protocol [20]. Global scope in this context means that all nodes within a segment routing domain add an entry in their Forwarding Information Base for the instruction associated with that segment [12]. The node identified by the node-SID is always reached by the shortest path, which is determined by the IGP algorithm [7]. That means an ingress node can impose a source route to a packet by specifying another node to be traversed by prepending the correspondent node-SID to that packet.

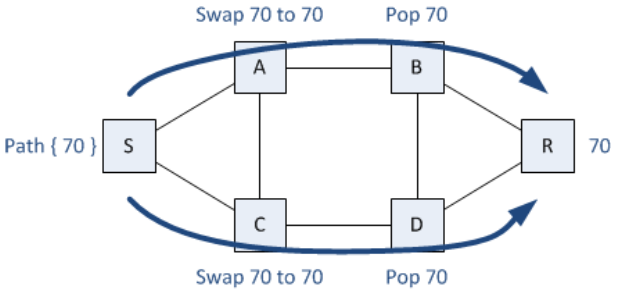

Figure 1: Node Segments [20]

Figure 1 shows an exemplary scenario: Node R advertised its node-SID 70 to all other nodes within the domain. Node S can instruct incoming packets to traverse node R by prepending the node-SID 70 to it. Hence the packet will be either forwarded via the path {S,A,B,R} or {S,C,D,R}, depending on which of both paths have been investigated as the shortest path. Intermediate nodes do not change the prepended SID, thus symbolically swapping it from 70 to 70, except for the last node. The last node on the path towards R is directly connected to R and thereby can remove the SID as this information is not needed anymore [20].

2.3.2 IGP-Prefix Segment

In fact, a nodal segment is a special case of an IGP-prefix segment, as a nodal segment represents a specific node by advertising a prefix of full address length [19]. In general a node can advertise the network prefixes it is attached to with the help of prefix segments, assigning a global segment identifier to each of them (referred to as prefix-SID) [7, 19]. Prefix segments are principally treated and forwarded the same way as explained in section 2.3.1 for nodal segments, with the difference that a certain prefix-SID is only advertised by those nodes that are attached to the respective (sub)network and thus can advertise a route to it within the IGP domain [19]. Prefix segments consequently also have global relevance within the segment routing domain [7].

2.3.3 IGP-Adjacency Segment

An IGP-Adjacency segment in turn has only local scope and thus is identified by a node-locally unique SID. A adjacency segment can be assigned to a specific unidirectional link that is directly attached to a node [7]. This type of segment is likewise advertised within the whole segment routing domain via the IGP protocol in use, but is only installed into the Routing Information Base (RIB) of remote nodes [21]. That means remote nodes can use the SIDs for imposing a route that steers a packet over specific links, but do not install an forwarding entry in their own Forwarding Information Base (FIB) [21]. The latter is only done by the node that advertises the adjacency segment [7].

Multiple SIDs of different types can be stacked and all SIDs together compose the path to be traversed. The imposed

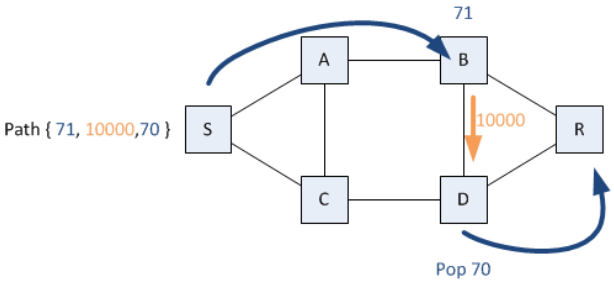

Figure 2: Node and Adjacency Segments [20]

path can either be fully explicit and complete, or define portions of the path while the regular shortest-path algorithm determines the rest of the path [7, 20]. Figure 2 shows combined usage of an adjacency and nodal segments: Node B installed an adjacency segment with SID 10000 in its FIB and advertised it to all other nodes. Additionally node B is also allocating a nodal segment with SID 71. Node R is also allocating a nodal segment with SID 70. An ingress node S can steer packets over the path {S,A,B,D,R} to reach node R by prepending the SIDs {71,10000,70}. Firstly, SID 70 steers packets to node B via shortest-path-first, SID 10000 then causes packets to be forwarded through the directly attached link to node D, and node D is forwarding packets towards R because of SID 70 [20].

2.4 Implementation via MPLS

The implementation of segment routing using the MPLS data plane is pretty straight forward as the forwarding plane is kept unmodified [9]. Since MPLS is a label switching mechanism, it already offers labels that can be used to represent and encode the SIDs [9]. MPLS also offers to stack labels, which allows to stack multiple segment identifiers. It also defines appropriate operations to process and to manipulate the label stack, such as push, pop and swap [5]. The currently active segment to be processed is always considered to be the top of the label stack, with the next segments below accordingly [9]. The main difference between pure MPLS and MPLS for segment routing is, that segment routing does not depend on any additional label distribution protocols such as LDP or RSVP and thus reduces operational complexity. Only the IGP (OSPF or IS-IS) is needed, which is in use either way [9].

2.5 Implementation via IPv6

The motivation for an additional IPv6-only based implementation of the segment routing mechanism is, that some network operators cannot or wish not to deploy MPLS in their IPv6 network [22]. An IPv6-only implementation can be in favor of an easier network administration, a lack of MPLS-enabled hardware or simply better scalability then offered by MPLS label [22]. For more details, this IETF draft "IPv6 SPRING Use Cases" [22] explaines some IPv6-only use cases of segment routing.

Segment routing functionality is added to IPv6 by a new routing extension header of type 4, called *Segment Routing Header (SRH)*. As illustrated in Figure 3, the SRH carries a list of SIDs [8]. SIDs are encoded as IPv6 addresses instead of labels as it is the case when using MPLS. The IPv6 address of a segment routing node serves as node-SID, whereas an adjacency-SID can be any global or local IPv6 address that is not already in use [8]. When reaching the ingress node of a segment routing domain, the original IPv6 datagram is encapsulated with an outer IPv6 header and the SRH [8]. The currently active SID is always copied into the destination address field of the new outer standard IPv6 header, and is further located within the segment list contained in the SRH by the index in the *Segments Left* field [8]. The *Policy List* fields in the SRH are optional and might for example indicate the ingress router at which the packet entered the segment routing domain or the egress router at which the packet is ought to leave the segment routing domain [8].

2.6 Security Considerations

The segment routing architecture assumes a basic trust model: Any node imposing a segment routed path to a packet is legitimate to do so [2]. Hence the operator of a segment routing enabled network has to ensure that all participating nodes within the segment routing domain are trustworthy and are not compromised by malicious evildoers [8]. Furthermore the IPv6-only implementation offers the opportunity to authenticate the segment routing header by an optional HMAC signature field. Consequently, within domains that strictly protect and apply the pre-shared secret key for HMAC computation, no attackers can impersonate as legitimate segment routing nodes [8]. Moreover, RFC 7785 [2] explicitly mandates that a segment routing implementation *"MUST NOT expose any source-routing information when a packet leaves the trusted domain"* and should filter incoming packets from outside the domain that carry segment routed paths [2].

3. ALTERNATIVE SOURCE ROUTING SOLUTIONS

Besides the IETF SPRING working group's standardization efforts, several other source routing solutions exist. A selected set of wellknown and commonly used mechanisms is presented in this chapter. However the heterogeneity of these techniques with regard to efficiency, scalability and maintainability highlights the need of a universal solution. The development of the latter is subject to the SPRING working group.

3.1 Obsolete IPv6 RH0 Extension Header

The Internet Protocol Version 6 defines a source routing mechanism that can be optionally applied by an routing extension header of type 0 (short: RH0) [3]. The extension header allows to define an arbitrary list of non-multicast IPv6 addresses that need to be transitted before reaching the last address of the list, which is representing final destination [3]. The length of this list is only limited by the *Maximum Transmission Unit (MTU)* and the resulting maximum packet size [23].

This routing extension header of type 0 has been deprecated by the IETF due to security concerns and thus is filtered by the majority of routers and firewalls [24]. The fact that the list of addresses can contain arbitrary (non-multicast) entries allows for addresses to appear multiple times. As worst

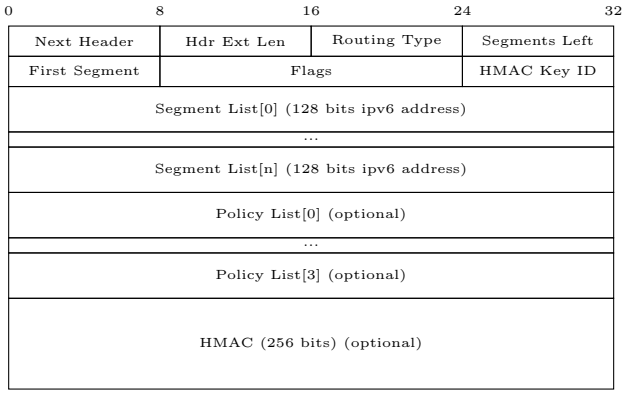

Figure 3: IPv6 Segment Routing Header

case this circumstance can be abused to keep packets travelling between two nodes, consuming bandwidth, switching capacity and processing power on all nodes along this cyclic path [24]. The routing header can thereby be used by attackers to compose *Denial of Service (DoS)* attacks with high efficiency; injected traffic is amplified many times as RH0 enables packets to be routed back and forth [24].

3.2 MPLS with RSVP or LDP

Huge networks that are operated and administrated by a central organizational unit, such as internet service provider networks, extensive company networks or content delivery networks, are often optimized and strengthened by traffic engineering policies. Up to now MPLS is the method of choice to accomplish traffic engineering via source routing [22]. Dedicated protocols such as the *Label Distribution Protocol (LDP)* and *Resource Reservation Protocol (RSVP)* are necessary to communicate label meanings and establish per-flow states on all nodes along a path [25]. Each unidirectional flow needs a label-switched path to be configured on MPLS nodes (called tunnel), i.e. new flow-dependent labels are installed on all MPLS routers on the path from the head-end towards the tail-end router [26]. Both protocols, LDP and RSVP, are used for building up and maintaining such tunnels, but signalization with LDP is limited to the IGP-based shortest-path-first routes, whereas RSVP uses a constrained SPF-algorithm and thus allows for more sophisticated and explicit path configuration [25].

3.3 Routing Protocol for Low-Power and Lossy Networks (RPL)

The *Routing Protocol for low-power and lossy networks (RPL)* is a routing protocol based on the distance-vector algorithm. It has been developed for networks that contain components which are limited in memory, bandwidth, energy and computational power [27]. It only supports IPv6 and helps reducing routing complexity for low-power routers by using the source routing paradigm. As result routers do not need to maintain extensive routing information bases as the path is already encoded in the IPv6 packet. Therefore RPL defines an IPv6 routing extension header of type 3 which carries a list of all next hop addresses needed to reach the final destination [27].

RPL only allows for strict hop-by-hop source routing and tunnels traffic by encapsulating the original incoming IPv6 datagram into a second outer IPv6 header (and its extension header), if the router is not the originator of the packet itself. If the latter is the case, the packet does not need be encapsulated into a second IPv6 header and the routing extension header is directly added to the original IPv6 header [27]. The destination IP address of the (outer) IP header represents the next hop to be visited and is switched to the next address upon reaching the designated next hop. It is important to note that RPL source routing headers have only significance within the RPL domain and must not be carried into other RPL domains [27].

3.4 Dynamic Source Routing (DSR) Protocol for Wireless Ad Hoc Networks

The *Dynamic Source Routing (DSR)* protocol is a self-organizing protocol that is well suited for wireless networks that operate adhoc and without designated infrastructure [28]. Topologies of such networks typically contain nodes located on opposite ends of the network and hence being out of direct range to each other. Such nodes are dependent on other nodes in between to forward packets originated by or destined for them [29]. Moreover, wireless adhoc networks often face high node mobility, thus including nodes that change their location within the network topology as well as occasionally quitting and entering the network [29].

DSR is a protocol that is self-adapting to topology changes by determining on-demand which paths are currently available towards the destination. A node discovers the path(s) to a target on-demand by a broadcasting a *Route Request* message to all neighboring nodes within transmission range. The request contains an ID as well as a list of IP addresses that were previously visited (initially empty) [28, 30]. Receiving nodes either discard the packet because they have received a request with the same ID before, broadcast it again within their transmission range while appending their IP address to the list of intermediate hops, or respond to it with a *Route Reply* message because they are the target of the request. The Route Reply is containing a copy of the list of intermediate hops. The final list that is sent with the Route Reply is used by the initiator of the request for imposing source routes to the packets destined for the target node [28, 30]. Discovered routes are cached in the routing information base and can be used for future packets until the path gets invalid and packets cannot be delivered. In this case the old route is removed from the routing table and a known alternative route is used, or a new route is discovered [28]. Various versions and extensions of DSR exist, offering additional quality properties and optimizations with regard to security [31, 32], energy efficiency [33], node-disjoint paths [34] and many more aspects.

4. DISCUSSION

Comparing the different source routing approaches presented above, the heterogeneity of these techniques with regard to efficiency, scalability and maintainability is remarkable. MPLS using LDP or RSVP for label distribution especially lacks easy maintainability due to complex protocol formats and complex interaction and synchronization of multiple

protocols [35, 36]. In addition RSVP lacks good scalability due to its point-to-point concept [37].The obsolete IPv6 RH0 extension header has no importance for today's networks any longer, as it was officially deprecated by the IETF and is filtered by most routers and firewalls. However it is mentioned in this proceeding because other solutions were inspired by it and learnt from that negative example with regard to security. The Dynamic Source Routing protocol is a well-suited solution for wireless adhoc networks and is also efficiently supporting node mobility [28]. Due to its on-demand approach the signaling overhead is reduced to only those routes that are actually requested [30]. Furthermore no periodic updates flood the network. The signaling overhead can be further reduced by caching not only routes retrieved from node-specific requests but also analyzing all Route Reply messages that have been provoked by other nodes. Moreover one single Route Request message discovers many alternative routes to the destination if present [30]. This results in excellent efficiency for topologies with low node mobility, while signaling overhead and outdated cache states rise with increasing node mobility [28].Segment Routing benefits the most of its seemless integration into both existing MPLS infrastructure and IPv6 networks. Because of its extensions for OSPF and IS-IS, segment routing requires no additional protocol other than the IGP that is already in use [9]. Therefore segment routing reduces the complexity of the source routing architecture and allows for simplified administration and maintenance of source routed network domains [38]. Providing the opportunity to steer traffic over specific links permits to use segment routing for efficient traffic engineering purposes. Furthermore the IPv6 implementation of segment routing offers authentication and integrity protection of the imposed source route via HMAC [8], which is not offered by MPLS, RPL or DSR by default.

In a nutshell, all mechanisms that encode the source route in packets have in common that the overhead per packet increases with the route length. On the other hand, mechanisms that do not encode the source route in packets but maintain per flow states on intermediate nodes tend to scale worse and require more memory and processing power on source-routing enabled network components.

5. CONCLUSION

With todays extensive and increasing usage of network infrastructure, source routing will become a key technology for large-scale networks in oder to optimize traffic flows and implement traffic policies. Especially with regard to content delivery networks and the associated tremendous amout of data to be exchanged, source routing will more and more become an important mean for an efficient allocation of infrastructure resources. The growth of giants like Youtube, Amazon, Netflix and many other multimedia streaming services and IPTV services indicate an outrageous network load that will increase even more and needs to be accommodated in future. Segment Routing is a promising technique that shows potential to establish an universal standard for source routing. Segment Routing seems to be an appealing technique for producers of networking hardware and network operators. The industrial interest in a unified and standardized source routing solution is quite obvious, as the IETF SPRING working group experiences broad support of huge companies such as Cisco, Nokia, Juniper and some more, which attend the working group's meetings or even send associates to contribute to the working group's activities.

The success of segment routing will largely depend on the security of this technology, because this has already been a deal-breaker in the past (just recall the abandoned IPv6 RH0 extension header). The future will show whether network operators succeed in preventing abuse through malicious attackers. Since backbone and provider networks have always been worthwhile targets for attackers as they offer the potential to paralyze or spy a large portion of the internet traffic, one can be sure that hackers will sound every security flaw that comes with segment routing. Considering the tremendous and continuously growing sizes of internet service provider networks or data center architectures, operating secure segment routing will be a challenging task. Especially with regard to an attacker from the inside of a segment routing domain, who is not restrained by the assumed basic trust model, but is quite likely due to many staff members, security will be a challenge to cope with.

6. REFERENCES

[1] L. L. Peterson and B. S. Davie, *Computer networks: a systems approach*. Elsevier, 2007.

[2] S. Previdi, C. Filsfils, B. Decraene, S. Litkowski, M. Horneffer, and R. Shakir, "Source Packet Routing in Networking (SPRING) Problem Statement and Requirements." RFC 7855 (Informational), May 2016.

[3] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification." RFC 2460 (Draft Standard), Dec. 1998. Updated by RFCs 5095, 5722, 5871, 6437, 6564, 6935, 6946, 7045, 7112.

[4] S. Krishnan, J. Woodyatt, E. Kline, J. Hoagland, and M. Bhatia, "A Uniform Format for IPv6 Extension Headers." RFC 6564 (Proposed Standard), Apr. 2012.

[5] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture." RFC 3031 (Proposed Standard), Jan. 2001. Updated by RFCs 6178, 6790.

[6] A. Retana and S. Bryant, "Charter: Source Packet Routing in Networking," 2013. `https://datatracker.ietf.org/doc/charter-ietf-spring/`; last accessed on 2016/12/20.

[7] C. Filsfils, S. Previdi, B. Decraene, S. Litkowski, and R. Shakir, "Segment Routing Architecture," 2016. `https://tools.ietf.org/html/draft-ietf-spring-segment-routing-10`; last accessed on 2016/12/19.

[8] C. Filsfils, S. Previdi, B. Field, and I. e. a. Leung, "IPv6 Segment Routing Header (SRH)," 2015. `https://tools.ietf.org/html/draft-previdi-6man-segment-routing-header-08`; last accessed on 2016/12/20.

[9] C. Filsfils, S. Previdi, B. Decraene, S. Litkowski, and R. e. a. Shakir, "Segment Routing with MPLS data plane," 2016. `https://tools.ietf.org/html/draft-ietf-spring-segment-routing-mpls-05`; last accessed on 2016/12/18.

[10] SPRING working group, "Status report for SPRING WG meeting on 2016-11-17," 2016. `https://www.ietf.org/proceedings/97/slides/slides-97-spring-0_ietf97_spring-wg-status-00.ppt`; last accessed on 2016/12/18.

[11] X. Xiao, A. Hannan, B. Bailey, and L. M. Ni, "Traffic Engineering with MPLS in the Internet," *IEEE network*, vol. 14, no. 2, pp. 28–33, 2000.

[12] Cisco Systems Inc., "Segment Routing: Prepare Your Network for New Business Models," 2015. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/application-engineered-routing/white-paper-c11-734250.html; last accessed on 2016/12/14.

[13] D. Awduche, A. Chiu, A. Elwalid, I. Widjaja, and X. Xiao, "Overview and Principles of Internet Traffic Engineering." RFC 3272 (Informational), May 2002. Updated by RFC 5462.

[14] Juniper Networks Corp., "Understanding VPWS," 2015. https://www.juniper.net/documentation/en_US/junos14.2/topics/concept/vpws-overview.html; last accessed on 2016/12/20.

[15] C. Filsfils, S. Previdi, B. Decraene, and R. Shakir, "SPRING Resiliency Use Cases," 2016. https://tools.ietf.org/html/draft-ietf-spring-resiliency-use-cases-08; last accessed on 2016/12/16.

[16] P. Psenak, C. Filsfils, R. Shakir, H. Gredler, W. Henderickx, and J. Tantsura, "OSPF Extensions for Segment Routing," 2015. https://tools.ietf.org/html/draft-ietf-ospf-segment-routing-extensions-10; last accessed on 2016/12/20.

[17] P. Psenak, C. Filsfils, R. Shakir, H. Gredler, W. Henderickx, and J. Tantsura, "OSPFv3 Extensions for Segment Routing," 2016. https://tools.ietf.org/html/draft-ietf-ospf-ospfv3-segment-routing-extensions-07; last accessed on 2016/12/19.

[18] S. Previdi, C. Filsfils, H. Gredler, S. Litkowski, B. Decraene, and J. Tantsura, "IS-IS Extensions for Segment Routing," 2016. https://tools.ietf.org/html/draft-ietf-isis-segment-routing-extensions-09; last accessed on 2016/12/20.

[19] S. Salsano, L. Veltri, L. Davoli, P. L. Ventre, and G. Siracusano, "PMSR-Poor Man's Segment Routing, a minimalistic approach to Segment Routing and a Traffic Engineering use case," *arXiv preprint arXiv:1512.05281*, 2015.

[20] Y. El Fathi, "Introduction To Segment Routing," 2013. http://packetpushers.net/introduction-to-segment-routing/; last accessed on 2016/12/20.

[21] D. Singh, "Yet Another Blog About Segment Routing - Part 1," 2015. http://packetpushers.net/yet-another-blog-about-segment-routing-part-1; last accessed on 2016/12/18.

[22] J. Brzozowski, J. Leddy, M. Townsley, C. Filsfils, and R. Maglione, "IPv6 SPRING Use Cases," 2016. https://tools.ietf.org/html/draft-ietf-spring-ipv6-use-cases-07; last accessed on 2016/12/20.

[23] B. Curtin, "Internationalization of the File Transfer Protocol." RFC 2640 (Proposed Standard), July 1999.

[24] J. Abley, P. Savola, and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6." RFC 5095 (Proposed Standard), Dec. 2007.

[25] Juniper Networks Corp., "Understanding the RSVP Signaling Protocol," 2013. https://www.juniper.net/documentation/en_US/junos12.1x47/topics/concept/mpls-security-rsvp-signaling-protocol-understanding.html; last accessed on 2016/12/20.

[26] D. Singh, "Yet Another Blog About Segment Routing - Part 3," 2015. http://packetpushers.net/yet-another-blog-segment-routing-part3-sr-te/; last accessed on 2016/12/18.

[27] J. Hui, J. Vasseur, D. Culler, and V. Manral, "An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)." RFC 6554 (Proposed Standard), Mar. 2012.

[28] D. B. Johnson, D. A. Maltz, J. Broch, *et al.*, "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks," *Ad hoc networking*, vol. 5, pp. 139–172, 2001.

[29] D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4." RFC 4728 (Experimental), Feb. 2007.

[30] B. Awerbuch, A. Mishra, and J. Hopkins, "Dynamic Source Routing (DSR) Protocol," *Johns Hopkins University, US*. http://www.cs.jhu.edu/~cs647/dsr.pdf; last accessed on 2016/12/20.

[31] F. Kargl, A. Geiß, S. Schlott, and M. Weber, "Secure Dynamic Source Routing," in *HICSS*, 2005.

[32] T. Jiang, Q. Li, and Y. Ruan, "Secure dynamic source routing protocol," in *Computer and Information Technology, 2004. CIT'04. The Fourth International Conference*, pp. 528–533, IEEE, 2004.

[33] M. Tarique, K. E. Tepe, and M. Naserian, "Energy saving dynamic source routing for ad hoc wireless networks," in *Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt'05)*, pp. 305–310, IEEE, 2005.

[34] J. Wu, "An extended dynamic source routing scheme in ad hoc wireless networks," *Telecommunication Systems*, vol. 22, no. 1-4, pp. 61–75, 2003.

[35] M. Jork, A. Atlas, and L. Fang, "LDP IGP Synchronization." RFC 5443 (Informational), Mar. 2009. Updated by RFC 6138.

[36] S. Kini and W. Lu, "LDP IGP Synchronization for Broadcast Networks." RFC 6138 (Informational), Feb. 2011.

[37] P. Lapukhov, "Scaling MPLS Networks," 2010. http://blog.ine.com/2010/08/16/scaling-mpls-networks/; last accessed on 2016/12/19.

[38] A. Korzh, "Segment-Routing." https://www.enog.org/presentations/enog-6/201-SR_ENOG.pdf; last accessed on 2016/12/20.