Why Internet Protocols Need Incentives

David Murray
School of Engineering and Information Technology
Perth, Western Australia
Email: D.Murray@murdoch.edu.au

***Abstract*—Internet routers are a commons. While modest regulatory measures have generally been successful for Information Communication Technologies (ICT), this paper argues that the lack of regulation has hindered the technological evolution of the Internet in some areas. This issue is examined through five Internet problems, and the technological solutions adopted. The key contribution of this paper is the explanation of these issues and the identification of areas where misaligned incentives promote inadequate solutions or inaction. The paper reviews the available measures to encourage the adoption of globally beneficial Internet technologies.**

***Keywords*—Internet Protocols, Protocol Drivers, Technology Policy**

I. Introduction

Since the inception of the Internet in the 1970's, the growth and rate of technological development in most areas has been rapid. The early 90's marked a turning point, where the Internet moved from being an academic network to a commercial network [1]. This commercialisation has generally been very successful, however, since 1993, certain key protocols have been difficult to change. This paper highlights where adoption has been constrained and it will discuss how the incentives are unlikely to encourage adequate long-term solutions.

This paper is concerned with the Internet infrastructure and the network protocols that keep it functioning as a transparent multi-purpose network. This Internet infrastructure is a commons, as packets may traverse a mixture of private and government owned routers and links on their way to their destination. The traditional view of commons, or Common Pool Resources (CPRs), is that they will inevitably be exploited [2]. More recent views on the long-term success of commons are less pessimistic [3] and the Internet is generally a prime example of an unregulated and successful commons.

One of the biggest differentiators between the Internet and traditional commons, such as grasslands or rivers, is that more Internet users do not necessarily lower other users' benefits. Some components of the Internet may improve due to Metcalfe's law. Despite the success of the Internet; operators, service providers and vendors, perhaps unknowingly, produce a series of economic externalities that are undesirable for the Internet's long term development.

An economic externality is a cost that is not included in the price of a good or service. Pollution is an obvious externality because the negative effects of pollution are not included in the price. Externalities commonly require government intervention. The regulation of Cloro-Fluro-Carbons (CFCs) and the requirement of catalytic converters in cars during the 1970s are both examples of successful government interventions. Pigouvian taxes, such as carbon taxes and emissions trading schemes, are more modern day examples of attempts to regulate economic externalities.

This paper will identify five different economic externalities in the Internet. The first externality, IPv6 adoption, is unanimously regarded as an exernality and thus numerous intervention strategies have been used to encourage support and adoption. The subsequent examples: DDoS, IP hijacks, fairness and stagnant MTUs present other areas which have not previously been identified as an externality. Although other issues, such as privacy and anonymity, are also obvious externalities, the technical topics, presented in this paper, have not previously been acknowledged as externalities and are poorly understood by policy makers.

II. IP Addressing Shortage

The number of users and devices on the Internet has increased dramatically. Given that the IPv4 address space is only 32-bits, and was inefficiently distributed, there has been a shortage of IPv4 addresses for some time. The Regional Internet Registry for the Asia Pacific region was the first to deplete its IPv4 pool in April 2011. In the same year, the first notable IPv4 trading occurred. Microsoft paid $7.5M USD to Nortel for over half a million IPv4 addresses [4], putting a market value of $11.25 per address. RIPE NCC ran out the following year in September 2012.

The most widely adopted solution to address shortages, is the adoption of Network Address Translation (NAT), which hides multiple devices behind a single global IP address. NAT violates the Internet's end-to-end layering principles because it changes IP addresses and port numbers on packets. Any NAT mechanism must understand the Transport protocol and thus the widespread adoption of new protocols such as Stream Control Transport Protocol (SCTP) and DCCP (Datagram Congestion Control Protocol), have become problematic as they are not widely supported by NAT [5]. As a result, the Internet is currently trapped into the use of TCP and UDP for end-to-end data transport.

The use of NAT has recently moved from the home broadband level to the carrier level. Carrier NATs have created further problems as many different households now share the same global IP address. Therefore, if one user launches a Denial of Service (DoS) or malicious attack on a popular website, then the use of an IP block will deny access to hundreds of users. The ideal solution to the shortage of IPv4 addresses is the widespread adoption of IPv6, as it would obviate the need for, and problems associated with, NAT.

The dependence on NAT as a solution has hampered the Internet's ability to adopt new transport layers, locking the

Internet into the use of TCP and UDP. The replacement of NAT with IPv6 would enable the use of significantly more robust Transport layers, such as SCTP. A principal benefit of SCTP is the ability to multi-home connections over multiple different interfaces. This substantially increases robustness in the presence of fading or intermittent wireless connections on mobile devices. Native IPv6 will also allow the use of DCCP which enables streamed HD video to detect network congestion.

Compliance with IPv6 is an externality. Service providers, network operators and equipment manufacturers have generally been slow to adopt IPv6 because it is only valuable if the rest of the Internet is setup for IPv6. Early adopters, of IPv6, have high private costs and, initially, low private benefits. Thus a cyclical problem forms: where each organisation waits and tries to externalise deployment costs until either crucially necessary, or a point where IPv6 is widespread. Consequently, the main addressing mechanism of the Internet, IPv4, has not drastically changed. The individualistic approach to address shortages, namely the adoption of NAT, has hindered the deployment and use of superior Transport protocols.

III. DDoS

DDoS attacks are caused by excessive illegitimate requests for resources. DDoS attacks are very hard to prevent as the symptoms of DDoS attacks are almost indistinguishable from heavy network demand [6]. In 2007, after Estonia relocated a Soviet monument, DDoS attacks from Russia crippled the websites of the Estonian parliament, banks, ministries, newspapers and broadcasters. The 2010 attacks on PayPal demonstrated that even the biggest and most well resourced organisations are at risk. These attacks were launched by groups that have access to thousands of compromised PCs or bots. They can use this network of bots or botnet, to target organisations. The number of requests for the service can consume the resources of legitimate users.

The current solution is for virus scanners to prevent hosts from being used as part of a DDoS botnet. After a DDoS has begun, the targeted organisation may also try to work with service providers to curtail offending hosts and links. This solution has not prevented DDoS attacks in the past and thus there is no certainty of improvement in the future.

DDoS attacks can also be amplified if the compromised hosts are able to spoof their source address. Therefore, DDoS attacks can be more easily performed if service providers do not performing address filtering.

A. Filtering Spoofed Addresses

IP address spoofing is the creation of Internet packets with a forged source IP address. It enables one host to appear as many hosts and increases the difficulty of identifying a machine launching a DDoS attack. Filtering source addresses is a best practice and is an interesting segue into the altruism of the Internet commons.

The act of filtering spoofed addresses prevents the network from sending spoofed packets, but does not provide protection from receiving spoofed packets. In 2009, a study found that 31% of Internet clients are able to spoof an arbitrary, routable source address and 77% of clients that are otherwise unable to do packet spoofing, can send packets from their own /24 network [7]. Longitudinal studies by Beverly et al [7], have demonstrated that there has been no improvement in the deployment of this Internet best practice [7].

Ideally, all Internet providers would conform to the best practice of address filtering. While attacks would still be possible from compromised hosts, address filtering would prevent the amplification of attacks. Unfortunately, the incentives to prevent DDoS attacks are inadequate. Currently, the only incentive to filter spoofed addresses is the knowledge that you are a good Internet citizen. Based on the evidence of poor address filtering adoption rates [7], these incentives are clearly inadequate.

B. Re-ECN

Another solution to this problem, that may have lacked the requisite attention, is Re-ECN [6]. This relatively recent IETF draft [8] enables the level of congestion being caused to be revealed to the whole network. While it was originally designed as a better way to control congestion, it is possible that, with the use of traffic policers in the core, it might be effective at preventing DDoS attacks [6]. This proposed DDoS preventative [6], is initially dependent on the adoption of Explicit Congestion Notification (ECN). ECN has not been widely adopted [9]. The details regarding ECN adoption will be further discussed later in this paper.

While parts of the Internet have adopted best practises and should be commended, many are still treating these functions as an externality and ignoring best practice. Active Queue Management (AQM) and ECN are essential before Re-ECN can reveal congestion throughout the network and thus, without incentive modification to increase adoption, these attacks will be viable in the foreseeable future. The adoption of Internet filtering and ECN are both changes that impose private costs and require a critical mass of adopters before any benefits are evident.

IV. IP Hijacks

IP hijacks, whether thorough nefarious intent or incompetence, have been occurring for some time. In 2003, Northrop Grumman's IP addresses were hijacked and used to send spam for over a month. In 2008, IP black holes were created during Pakistan's attempts to censor YouTube. This caused YouTube to be inaccessible, across the globe, for many hours. In 2010, a Border Gateway Routing Protocol (BGP) problem caused data to be misrouted through China, raising concerns over the security of misrouted data.

These problems have occurred through BGP. Route advertisements are accepted based on the trust of BGP peers. When a BGP router advertises a prefix, the peering router will *trust* that the Autonomous System (AS) is authorised to advertise the prefix and actually has a path to the destination [10].

To add sanity checks on what advertisements should or should not be trusted, some service providers *may* use route filtering and routing registries [11]. However, these mechanisms are known to be deficient [10]. These approaches are also only effective at the periphery of the Internet, where it

Website	Num Flows	Website	Num Flows
google.com	8	wikipedia.org	33
facebook.com	16	live.com	21
youtube.com	52	amazon.com	97
yahoo.com	75	qq.com	199
baidu.com	22	twitter.com	12

TABLE I. NUMBER OF TCP FLOWS USED BY A FIREFOX SESSION TO THE TEN MOST POPULAR WEBSITES

is administratively feasible to track what neighbours have the ability to advertise.

There have been numerous solutions to these issues. The majority of proposed solutions, such as SBGP [12], SoBGP and the more recent IETF BGPSec [13], rely on a Resource Public Key Infrastructure (RPKI). A certificate infrastructure will link the Autonomous System Number (ASN) and the IP address. The main goal is to validate whether an AS is authorised to advertise a IP range, as well ensuring that a valid path exists. These proposed end-to-end solutions have thus far been ignored in most operational networks.

Similar to IPv6, these RPKI based solutions require a critical mass before they are useful. Initial adopters will have high private costs and initially receive only marginal private benefits. Analogous to Internet address filtering, the RPKI authenticated networks will be more reliable and robust, however, those that have adopted this technology may still have their data mis-routed by other ISPs.

Given that the Internet is a general purpose network and supports a huge number of highly important daily functions, there is a massive collective benefit to increased robustness. The evidence suggests that the incentives, for those in the position to improve robustness, are inadequate [11]. Technological solutions exist, however, no new mechanisms, which can authorise whether a source has permission to advertise a certain IP range or determine whether the source has a valid path, have been adopted.

V. FAIRNESS

As the Internet has spread, fairness has become more complex. In theory, two flows traversing the same path should get an equivalent/fair share of bandwidth. However, to speed up Internet transactions, servers are opening many simultaneous TCP flows. Table I shows the number of TCP flows opened by the top 10 most visited websites. P2P file sharing applications, download accelerators and Torrents may have hundreds of long-term TCP flows [14]. The consequence of such misbehaviour is that, applications that are operating using the minimum number of TCP flows may experience reduced performance when competing against applications opening large numbers of TCP flows.

Opening larger numbers of TCP flows is an obvious externality. While it might increase the transfer speed between the sender and the receiver, it will also increase overheads, and obtain a more aggressive share of the bandwidth. Subsequently, it is questionable as to whether TCP flow fairness is still a useful goal [14].

To solve congestion problems, most ISPs either over-engineer links, use download caps or use traffic metering [15]. A sustainable, long-term solution is the adoption of Active Queue Management (AQM) and ECN. The most prominent Random Early Detection (RED) mechanism [16] has been well known for 20 years and has received over 6000 academic citations, however, the most recent reports still state that buffers are too big and that the deployment of AQM is absent [17].

Similar to RED, ECN was also proposed two decades ago. Currently, there is no evidence of Internet packets being marked with ECN Congestion Experienced (CE) flags [18], which suggests that ECN compliant AQM is completely absent.

There are a number of reasons why AQM and ECN have not been widely adopted. AQM mechanisms require tuning and testing to be successful [19]. Also, the capacity of a newly commissioned link might exceed demand and thus, during testing and deployment phases of a new link, the implementation of AQM might be unnecessary. While passive mode ECN has been implemented into modern host OS's, ECN compliant AQM mechanisms are required in routers to be effective. It is hoped that, a new AQM mechanism, known as Codel [19] may prove to be easier to implement and require less individual tuning, but Codel is only a subset of the solution.

Internet Transport protocols are also largely unchanged. Recent Internet measurement studies still show that the primary Transport protocols, namely TCP and UDP [20], have been the same for two decades. Relatively minor changes for example, Timestamps, Window Scaling and SACK, have occurred. Unfortunately, larger changes and new transport layers, such as SCTP and DCCP, are unusable over the majority of the Internet due to the existence of NAT.

VI. TOO MANY SMALL PACKETS

Link speeds have continually increased over the last 20 years, and will continue to do so in the foreseeable future. Fig 1 shows the number of bytes that traversed the Amsterdam Internet Exchange (AMS-IX), during the month of November, between 2001 and 2012. Table II shows the increase in Ethernet speeds over the past three decades. While link speeds have continually increased, the stagnant Maximum Transmission Unit (MTU) remains at 1500 bytes. Therefore every ten fold link speed increase required routers to process 10 times more packets. This increases CPU utilisation, power consumption and is an inefficient use of bandwidth - as an unnecessary proportion of data transmissions are also consumed by network headers [20].

The problems of increased CPU requirements and header overheads have been solved independently. WAN optimisers can reduce the header/bandwidth penalty of small packets [21]. The CPU problems of routing and header processing have also been solved in switches and routers with Application Specific Integrated Circuits (ASICs). TCP senders and receivers have adopted TCP Sender Offload (TSO) and Large Segment Offload (LSO). ASICs, TSO and LSO are mechanisms that shift processing from the CPU, to the network card. The commonality in all of these adopted solutions is that benefits are local and device specific rather than end-to-end and network specific.

The alternative solution to packet processing and overhead problems is to use a larger transmission unit. Increasing the

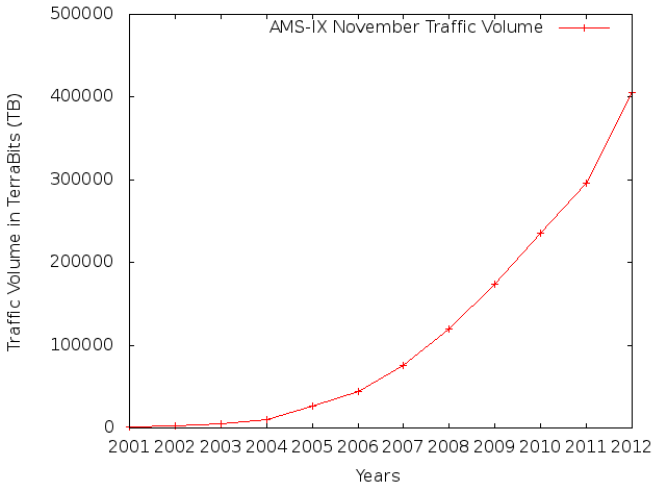

Fig. 1. Terrabits Bits (TB) Entering AMS-IX for the Month of November

MTU will simultaneously improve bandwidth efficiency, CPU cycles and power consumption [22]. The adoption of a more flexible MTU would enable devices to use the most appropriate transmission unit for the particular connection and conditions.

Small packets also have many negative implications for wireless traffic. Although larger packets may increase the chance of error, small packets greatly increase overheads in modern wireless networks [23]. The evidence of this is the standardisation of packet aggregation over 802.11n and 802.11ac networks. Packet aggregation will combine multiple 1500 byte frames for transmission over a wireless link. Increasing the MTU would eliminate the need for packet aggregation, which is known to substantially increase delays [24]. The use of larger packets also has benefits to the initial slow start stages of TCP [9] as well as for data centre applications such as file transfers, Hadoop and MapReduce [25].

Mindful that there is significant research effort and attention on new mechanisms to reduce the level of end-to-end buffering [17], the use of packet aggregation to overcome the inefficiencies of small transfer units is counter productive to major research goals. Packet aggregation in 802.11n and 802.11ac is another local solution to a problem that may be better solved by raising the MTU throughout the Internet.

The adoption problems for larger MTUs are consistent with all the adoption problems in this paper. Support must exist end-to-end before benefits are evident. Being among the first large MTU equipment manufacturers or the first providers to adopt a larger size *initially* imposes a large private cost with a marginal private benefit. Despite studies that have demonstrated the performance benefits of larger MTUs [9], Table II shows that the *mandatory* MTU in the Ethernet standard has not changed since the creation of Ethernet in 1982. The use of frame aggregation in wireless links is analogous to the use of NAT to solve IPv6. It provides an instant solution at that point on the Internet without addressing the underlying problem. Subsequently, traditional market forces are not producing a positive effect on technology development in this area.

TABLE II. ETHERNET STANDARDS AND THE MANDATORY MTUS

Technology	Data Rate	Year	MTU	Serialization Delay
Ethernet	10-Mb/s	1982	1500	1200-μs
Fast Ethernet	100-Mb/s	1995	1500	120-μs
Gig Ethernet	1,000-Mb/s	1998	1500	12-μs
10-Gig Ethernet	10,000-Mb/s	2002	1500	1.2-μs
100-Gig Ethernet	100,000-Mb/s	2010	1500	0.12-μs

VII. THE NEED FOR MARKET INTERVENTION

The previously discussed issues are externalities. The market forces are analogous to catalytic converters in cars. Catalytic converters are an example of a technology with initially high private costs and low private benefits.

Without government mandates for catalytic converters, consumers would have been reluctant to pay a premium for a car with only marginal health benefits to the owner. Without a mandate, manufacturers may have been unlikely to develop the technology or achieve economies of scale in production. For any scenario with high private costs and low private benefits, there is no rational economic motive to opt in, even if the collective benefits are high. The following is a summary:

1) Despite a clear need to adopt IPv6, the major IP addressing scheme has not changed since 1974. Furthermore, the widespread use of NAT has hindered the adoption of new Transport layer protocols such as SCTP and DCCP. Despite the global benefits, the adoption of IPv6 will initially have high private costs and low private benefits.
2) Rampant DoS and IP Hijacks have not improved the levels of ISP address filtering [7] or the adoption of secure enhancements to BGP. Although many of these problems could be alleviated with route filtering, registries [11] and IETF BGPSec [13], the high private costs and low private benefits leaves no rational economic motivation.
3) The mechanism to fairly allocate bandwidth has not substantially changed since 1988 [26], even though flow based fairness is now clearly suboptimal.
4) Despite recent evidence highlighting the importance of AQM and ECN [19], adoption in real world networks is largely absent [9].
5) The MTU of the Internet has not changed since 1982, despite the increasing complexity of header processing and overheads. While it is feasible for any organisation to create a Jumboframe capable network, doing so in isolation will yield significantly higher costs than benefits. The research suggests that the benefits from the adoption of Jumboframes are large [20], [25].

This paper argues that the Internet infrastructure is a common pool resource and that participants will operate and provide services as long as it aligns with their objectives, including profit motives and needs. The issues listed are unique because widespread adoption is necessary before benefits can be derived. The initial adopters are also likely to face the highest private costs and the lowest private benefits. This is a classic economic rationale for market intervention.

VIII. Market Intervention

Generally, the ICT industry has been spectacularly successful when operating with minimal bureaucratic or government intervention. At best, regulation is assumed to "get in the way" and limit creativity. At worst, high level meetings, such as WCIT-12, are contentious due to ambiguity over matters effecting anonymity and charging models.

This paper argues that public and private organisations should incentivise development in directions that might enable more technological freedom. Many governments throughout the globe have attempted to embrace open document formats and open standards. Incentivising the use of technological approaches that promote flexibility and architectural openness, is a similar goal. The following section lists and describes the current mechanisms available to promote positive externalities in the Internet.

A. Procurement

Governments are enormous users and consumers of networks; and procurement strategies can exert a great deal of market influence. DeNardis [27] suggests that Governments are obligated to have procurement policies that generate a number of positive network externalities. These organisations could, enable IPv6, AQM and ECN internally, purchase Jumboframe supported hardware and only use ISPs that will filter spoofed addresses.

B. Government Mandates and Targets

Governments can mandate compliance on all publicly owned and run infrastructure by a certain date. Government mandates were used for Y2K compliance. They are also currently being used in the US, Japan, Korea and Australia for IPv6 Compliance [28]. Mandates or pigovian taxes on private organisations are more difficult due to the international and border-less nature of the Internet. The bureaucratic overheads of checking and compliance are also difficult and costly.

C. Best Practice and Discussion Groups

Best practice guides and freely available configuration and conformance information may reduce the cost of collective migration to these schemes. The IETF has a series of Best Current Practice RFC's, however, they have not received recent updates and are not unanimously followed. There are groups of operators, such as North American Network Operators' Group (NANOG) and IPBCOP, however they only represent a subset of global operators.

D. Publishing Compliance and Non-Compliance

Compliance and non-compliance can be encouraged by publishing monthly online summaries. This 'name and shame' mechanism is currently implemented at cidr-report.org [29], where poor route aggregation techniques and possible 'bogons' are listed. As many of the network features discussed in this paper can be tested without the need for human intervention, these methods could be economically viable ways of promoting compliance.

E. Compliance Days/Conferences

Annual conformance days can promote collective compliance. Conferences can be held soon after to discuss implementation problems. Organisations running successful trials, may be tempted to leave their newly compliant areas of the network online. This concept has been successfully trialled with 'World IPv6 Day'. As a result, many organisations, such as Google, Yahoo, Bing, Facebook, and Cisco left IPv6 enabled following successful trials.

F. Government Ratings and Certification

A more aggressive form of market intervention, is a technical certification and ratings body. The use of ratings has been successful in increasing car safety standards. Consumers are made aware of a potential cars safety while hiding the technical details behind a rating number. Providing a similar rating scheme for Service Providers may re-balance the incentives and increase compliance. The mechanisms to certify or rate ISPs and the levels of bureaucracy to implement such a scheme would be large.

The use of certification bodies are used frequently throughout the IT industry. Restriction of Hazardous Substances Directive (ROHS) has been used to designate compliance with the use of non-hazardous substances. The WiFi Alliance and the Ethernet Alliance will test technical compliance with IEEE standards and relay this information in the form of a single logo to consumers. These certification or rating levels can inform consumers and create the correct economic incentives.

G. Appropriate Action

Many of the end-to-end solutions for the problems discussed are technically simple or widely available. In many cases the solution has existed for many years and is already being used by a small portion of the Internet. While the solution might be technically straightforward, orchestrating the solution across equipment vendors, end-users, and service providers is very difficult.

Evaluating which policy or approach promotes the best outcomes for the lowest cost is fraught with problems. Although 'World IPv6 Day' appears to have been successful, it is impossible to know if a 'World ECN Day' would be more or less successful. Furthermore, discussions about which intervention might yield the highest levels of conformance are only appropriate once widespread acceptance of these externalities has been reached. It is important to note that none of the listed strategies have been employed to promote Jumboframes, address filtering, ECN, RED or IETF BGPSec,

IX. Conclusion

This paper has reviewed five major issues where the incentives for rational actors to adopt globally beneficial solutions are misaligned. High private costs and low private benefits have resulted in the adoption of poor solutions to Internet problems. More specifically, individual or local solutions as opposed to end-to-end solutions have been preferentially adopted. Since 1993, when the Internet rapidly commercialised, the adoption of certain protocols has been constrained, and the incentives are inadequate to encourage optimal long term solutions.

REFERENCES

[1] M. Handley, "Why the internet only just works," *BT Technology Journal*, vol. 24, pp. 119–129, July 2006.

[2] G. Hardin, "The tragedy of the commons," *Journal of Natural Resources Policy Research*, vol. 1, no. 3, pp. 243–253, 2009.

[3] E. Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge University Press, 1990.

[4] A. Dul, "Economics of IPv4 Transfer Market on IPv6 Deployment." Online: www.quark.net/docs/Economics_of_IPv4_on_IPv6.pdf, 2011.

[5] D. Hayes, J. But, and G. Armitage, "Issues with network address translation for SCTP," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 1, pp. 23–33, 2008.

[6] B. Briscoe, "Using self-interest to prevent malice; Fixing the denial of service flaw of the Internet," in *Proc Workshop on the Economics of Securing the Information Infrastructure*, Oct. 2006.

[7] R. Beverly, A. Berger, Y. Hyun, and k claffy, "Understanding the efficacy of deployed internet source address validation filtering," in *Proceedings of the Ninth ACM SIGCOMM/USENIX Internet Measurement Conference (IMC)*, Nov. 2009.

[8] B. Briscoe, A. Jacquet, T. Moncaster, and A. Smith, "Re-ECN: Adding Accountability for Causing Congestion to TCP/IP." IETF Internet Draft, 2010.

[9] D. Murray, T. Koziniec, K. Lee, and M. Dixon, "Large MTUs and Internet Performance," in *IEEE 13th Conference on High Performance Switching and Routing*, pp. 390–401, 2012.

[10] K. Butler, T. Farley, P. McDonald, and J. Rexford, "A Survey of BGP Security Issues and Solutions," *Proceedings of the IEEE*, vol. 98, no. 1, p. 96, 2010.

[11] P. Trimintzios, C. Hall, R. Clayton, R. Anderson, and E. Ouzounis, "Resilience of the Internet Interconnection Ecosystem ." European Network and Information Security Agency (ENISA), 2011.

[12] S. Kent, C. Lynn, and K. Seo, "Secure border gateway protocol (S-BGP)," *Selected Areas in Communications*, vol. 18, no. 4, pp. 582–592, 2000.

[13] M. Lepinski, "BGPSEC Protocol Specification." IETF Draft: draft-ietf-sidr-bgpsec-protocol-05, 2012.

[14] B. Briscoe, "Flow rate fairness: dismantling a religion," *SIGCOMM Comput. Commun. Rev.*, vol. 37, pp. 63–74, Mar. 2007.

[15] I. Society", "Bandwidth management," *Internet Society Technology Roundtable Series*, November 2012.

[16] S. Floyd and V. Jacobson, "Random early detection gateways for congestion avoidance," *IEEE/ACM Trans. Netw.*, vol. 1, pp. 397–413, Aug. 1993.

[17] J. Gettys and K. Nichols, "Bufferbloat: Dark buffers in the internet," *Internet Computing, IEEE*, vol. 15, p. 96, may-june 2011.

[18] A. Medina, M. Allman, and S. Floyd, "Measuring the evolution of transport protocols in the internet," *ACM Computer Communication Review*, 2005.

[19] K. Nichols and V. Jacobson, "Controlling queue delay," *Queue*, vol. 10, pp. 20:20–20:34, May 2012.

[20] D. Murray and T. Koziniec, "The State of Enterprise Network Traffic in 2012," in *Proceedings of The 18th Asia-Pacific Conference on Communications*, (APCC 2012), IEEE, 2012.

[21] Riverbed, "Riverbed Optimization System." Online: www.riverbed.com/docs/TechOverview-Riverbed-RiOS.pdf, 2012.

[22] S. Makineni and R. Iyer, "Architectural Characterization of TCP/IP Packet Processing on the Pentium 4; M Microprocessor," in *Proceedings of the 10th International Symposium on High Performance Computer Architecture*, (Washington, DC), IEEE Com Soc, 2004.

[23] H. Falaki, D. Lymberopoulos, R. Mahajan, S. Kandula, and D. Estrin, "A first look at traffic on smartphones," in *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*, IMC '10, (New York), pp. 281–287, ACM, 2010.

[24] B. Bellalta, J. Barceló, D. Staehle, A. V. Vinel, and M. Oliver, "On the Performance of Packet Aggregation in IEEE 802.11ac MU-MIMO WLANs," *CoRR*, 2012.

[25] P. Prakash, M. Lee, Y. C. Hu, and R. R. Kompella, "Jumbo frames or not: That is the question!," 2013.

[26] V. Jacobson, "Congestion avoidance and control," in *ACM SIGCOMM Computer Communication Review*, vol. 18, pp. 314–329, ACM, 1988.

[27] L. DeNardis, "E-governance policies for interoperability and open standards," *Policy & Internet*, vol. 2, no. 3, pp. 129–164, 2012.

[28] Organisation for Economic Co-operation and Development (OECD), "Internet Address Space: Economic Considerations in the Management of IPv4 and in the Deployment of IPv6." OECD Ministerial Meeting, 2008.

[29] T. Bates, P. Smith, and G. Huston, "CIDR Report." Online: www.cidr-report.org/as2.0/, 2013.