Network Working Group
Internet-Draft
Expires: November 6, 2017

N. Rooney
GSMA

May 5, 2017

IAB Workshop on Managing Radio Networks in an Encrypted World (MaRNEW) Report
draft-nrooney-marnew-report-03

Abstract

The MarNEW workshop aimed to discuss solutions for badnwidth optimisation on mobile networks for encrypted content, as current solutions rely on unencrypted content which is not indicative of the security needs of today's internet users. The workshop gathered IETF attendees, IAB members and various organisations involved in the telecommunications industry including original equipment manufacturers and mobile network operators.

The group discussed the current internet encryption trends and deployment issues identified within the IETF, and the privacy needs of users which should be adhered. Solutions designed around sharing data from the network to the endpoints and vice versa were then discussed as well as analysing whether the current issues experienced on the transport layer are also playing a role here. Content providers and CDNs gave an honest view of their experiences delivery content with mobile network operators. Finally, technical responses to regulation was discussed to help the regulated industries relay the issues of impossible to implement or bad-for-privacy technologies back to regulators.

A group of suggested solutions were devised which will be discussed in various IETF groups moving forward.

This Internet-Draft will expire on November 6, 2017.

1. Introduction

Mobile networks have a set of requirements and properties which places a large emphasis on sophisticated bandwidth optimization. Encryption is increasing on the internet which is positive for consumer and business privacy and security. Many existing mobile bandwidth optimization solutions primarily operate on non-encrypted communications; this can lead to performance issues being amplified on mobile networks. Encryption on networks will continue to increase; and with this understanding the workshop aimed to understand how we can solve the issues of bandwidth optimization and performance on radio networks in this encrypted world.

1.1. Understanding "Bandwidth Optimization"

For the purposes of this workshop, bandwidth optimization encompasses a variety of technical topics related to traffic engineering, prioritisation, optimisation, efficiency enhancements, as well as user-related topics such as specific subscription or billing models. These can include:

- Caching
- Prioritisation of interactive traffic over background traffic
- Per-user bandwidth limit
- Business-related topics such as content delivery arrangements with specific content providers.

Many of these functions can continue as they're performed today, even with more encryption. Others use methods which require them to inspect parts of the communication that are encrypted, and these will have to be done differently in an encrypted Internet.

Finally, while not strictly speaking traffic management, some networks employ policy-based filtering (e.g., requested parental controls) and all networks support some form of legal interception functionality per applicable laws.

1.2. Topics

The workshop aimed to answer questions including:

- Understanding the bandwidth optimization use cases particular to radio networks
- Understanding existing approaches and how these do not work with encrypted traffic
- Understanding reasons why the Internet has not standardised support for lawful intercept and why mobile networks have
- Determining how to match traffic types with bandwidth optimization methods
- Discussing minimal information to be shared to manage networks but ensure user security and privacy
- Developing new bandwidth optimization techniques and protocols within these new constraints
- Discussing the appropriate network layer(s) for each management function
- Cooperative methods of bandwidth optimization and issues associated with these

The further aim was to gather architectural and engineering guidance on future work in the bandwidth optimisation area based on the discussions around the proposed approaches. The workshop also explored possible areas for standardization, e.g. new protocols that can aid bandwidth optimization whilst ensuring user security inline with new work in the transport layer.

1.3. Organization of this report

This workshop report summarizes the contributions to and discussions at the workshop, organized by topic. The workshop began with scene setting topics which covered the issues around deploying encryption, the increased need for privacy on the internet and setting a clear understanding that ciphertext should remain unbroken. Later sessions focused on key solution areas; these included evolution on the transport layer and sending data up or down the path. A session on application layers and CDNs aimed to highlight both issues and solutions experienced on the application layer. The workshop ended with a session dedicated to technical response to regulation with regards to encryption. The contributing documents were split between identifying the issues experienced with encryption on radio networks and suggested solutions. Of the solutions suggested some focused on transport evolution, some on trusted middleboxes and others on collaborative data exchange. Solutions were discussed within the sessions. All accepted position papers and detailed transcripts of discussion are available at [MARNEW].

The outcomes of the workshop are discussed in Section 7 and 8, and discuss progress after the workshop toward each of the identified work items as of the time of publication of this report.

Although policy related topics were out of scope for this workshop they were infrequently referred to. Report readers should be reminded that this workshop did not and did not aim to discuss policy or policy recommendations.

1.4. Use of Note Well and Charter House Rule

The workshop was conducted under the IETF [NOTE_WELL] with the exception of the "Technical Analysis and Response to Potential Regulatory Reaction" session which was conducted under [CHATHAM_HOUSE_RULE].

1.5. IETF and GSMA

The IETF and GSMA [GSMA] have divergent working pratices, standards and processes. IETF is an open organisation with community driven standards with the key aim of functionality and security for the internet's users, the GSMA is membership based and serves the needs of its membership base most of whom are mobile network operators.

Unlike IETF, GSMA makes few standards. Within the telecommunications industry standards are set in various divergent groups depending on their purpose. Perhpas of most relevance to the bandwidth optimisation topic here is the work of the [SDO_3GPP] which work on

radio network and core network standards with their members which include mobile operators and original equipment manufacturers.

One of the [SDO_3GPP] standards relevant to this workship is PCC-QoS [PCC-QOS]. Traditionally mobile networks have managed different applications and services based on the resources available and priorities given; for instance, emergency services have a top priority, data has a lower prioirty and voice services are somewhere inbetween. [SDO_3GPP] defined the PCC-QoS mechanism to support this functionality, some of which cannot occur for encrypted communications.

2. Scene Setting Sessions

Scene setting sessions aimed to bring all attendees up to a basic understanding of the problem and the scope of the workhop. There were three scene setting sessions: Scene Setting (defining scope), Encryption Deployment Considerations and Trust Models and User Choice (Privacy).

2.1. Scene Setting

The telecommunications industry and internet standards are extremely different in terms of ethos and business practices. Both industries drive technical standards in their domain and build technical solutions with some policy-driven use cases. These technologies, use cases and technical implementations are different; not only this but motivators between the two industries are also diverse.

To ensure all attendees were aligned with contributing to discussions and driving solutions this "Scene Setting" session worked on generating a clear scope with all attendees involved. In short: it was agreed that ciphertext should not be broken by any solution, that the radio access network (RAN) is different and does experience issues with increased encrypted traffic, that we need to understand what those problems are precisely and that our goal is to improve user experience on the Internet. Technical solutions for regulation was not in scope. The full scope is given below.

2.1.1. Scope

The attendees identified and agreed the following scope:

- In discussion we should assume: No broken crypto, Ciphertext increasingly common, congestion does need to be controlled as do other transport issues and Network management including efficient use of resources, in RAN and elsewhere, has to work

- How/why is RAN different for transport; help us understand the complexities of the RAN and how hard it is to manage and why those matter

- What are the precise problems caused by more ciphertext

- Identify players, incl. Users, and resulting tensions and how ciphertext changes those

- Some solutions will be radically changed by ciphertext, it's ok to talk about that

- As good as possible Quality of experience for end user is a goal

- Our aim for the next two days is to analyse the situation and identify specific achievable tasks that could be tackled in the IETF or GSMA (or elsewhere?) and that improve the Internet given the assumptions above

- We should not delve into:

- Ways of doing interception (legal or not), see RFC2804 for why

- Unpredictable political actions.

2.1.2. Encryption Statistics and Radio Access Network Differences

Attendees were shown that encrypted content is reaching around 50% according to recent statistics [STATE_BROWSER] and [STATE_SERVER]. The IAB are encouraging all IETF groups to consider encryption by default on their new protocol work and the IETF are also working on encryption on lower layers, for example TCP encryption within the [TCPINC] Working Group. The aims of these items of work are greater security and privacy for users and their data.

Within telecommunications middleboxes exist on operator networks which have previously considered themselves trusted; but qualifying trust is difficult and should not be assumed. Some interesting use cases exist with these middleboxes; such as anti-spam and malware, but these need to be balanced against their ability to open up cracks in the network for attacks such as pervasive monitoring. Some needs to improve the radio access network quality of service could come from increasing radio access network cells ("Base Stations"), but this adds to radio pollution; this shows the balancing act when deivising radio access network architecture.

2.2. Encryption Deployment Considerations

Encryption across the internet is on the rise. However, some organisations and individuals come across a common set of operational issues when deploying encryption, mainly driven by commercial perspectives. The [UBIQUITOUS] draft explains these network management function impacts, detailing areas around incident monitoring, access control management, and regulation on mobile networks. The data was collected from various internet players, including system and network administrators across enterprise, governmental organisations and personal use. The aim of the document is to gain an understanding of what is needed for technical solutions to these issues, maintaining security and privacy for users. Attendees commented that worthwhile additions would be: different business environments (e.g. cloud environments) and service chaining. Incident monitoring in particular was noted as a difficult issue to solve given the use of URL in today's inicident monitoring middleware.

Some of these impacts to mobile networks can be resolved using difference methods and the [NETWORK_MANAGEMENT] draft details these methods. The draft focuses heavily on methods to manage network traffic whithout breaching user privacy and security.

By reviewing encryption depoyment issues and the alternative methods of network management MaRNEW attendees were made aware of the issues which affect radio networks, the deployment issues which are solvable and require no further action, and those which aren't currently solveable and which should be addressed within the workshop.

2.3. Trust Models and User Choice (Privacy)

Solutions of how to improve delivery of encrypted content could affect some of all of the privacy benefits that encryption brings. Understanding user needs and desires for privacy is therefore important when designing these solutions.

From a recent study [Pew2014] 64% of users said concerns over privacy have increased, 67% of mobile internet users would like to do more to protect their privacy. The W3C and IETF have both responded to user desires for better privacy by recommending encryption for new protocols and web technologies. Within the W3C new security standards are emerging and the design principles for HTML hold that users are the stakeholders with most priority, followed by implementors and other stakeholders, further inforcing the "user first" principle. Users also have certain security expectations from particular contexts, and sometimes use new technologies to further

protect their privacy even if those technologies weren't initially developed for that purpose.

Technologies which can impact user privacy sometimes do this ignorant of the privacy implications or incorrectly assume that the benefits users gain from the new technology outweigh the loss of private information. Any new technology which introduces bad security vectors will be used by attackers. If these technologies are necessary they should be opt-in.

Internet stakeholders should understand the priority of other stakeholders. Users should be considered the first priority, other stakeholders include implementors, developers, advertisers, operators and other ISPs. Some technologies have been absued by these parties, such as cookie use or JavaScript injection. This has caused some developers to encrypt content to circumnavigate these technologies which they find intrusive or bad for their users privacy.

Some suggested solutions for network management of encrypted traffic have suggested "trust models". If users and content providers are to opt-in to user network management services with negative privacy impacts they should see clear value from using these services, and understand the impacts on clear interfaces. Users should also have easy abilities to opt-out. Some users will always automatically click through consent requests, so any trust model is flawed for these users. Understanding the extent of "auto click through" may help make better decisions for consent requests in the future. One trust model (Cooperative Traffic Management) works as an agent of the user; by opting-in metadata can be shared. Issues with this involve trust only being applied on end.

3. Network or Transport Solution Sessions

Network or Transport Solution Sessions aimed to discuss suggested and new solutions for managing encrypted traffic on radio access networks. Most solutions focus on the sharing of metadata; either from the enpoint to the network, from the network to the endpoint, or cooperative sharing between both. Evolutions on the transport layer could be another approach to solve some of the issues radio access networks experience which cause them to require network management middleboxes. By removing problems on the transport layer the need to expesnive middleboxes could decrease.

3.1. Sending Data Up / Down for Network Management Benefits

Middleboxes in the network have a number of uses, some which are more beneficial than they are controversial. Collaboration between these

network elements and the endpoints could bring about better content distribution. A number of suggestions were given, these included:

- Mobile Throughput Guidance [MTG]: exchanges data between the network elements and the endpoints via TCP Options. It also allows for gaining a better idea of how the transport protocol behaves and improving user experience further, although the work still needs to evolve.

- SPUD [SPUD]: a UDP-based encapsulation protocol to allow explicit cooperation with middleboxes while using new, encrypted transport protocols.

- Network Status API: An API for operators to share congestion status or the state of a cell before an application starts sending data could allow applications to change their behaviour.

- Traffic classification: classfying traffic and adding this as metadata for analysis throughout the network. This idea has trust and privacy implications.

- ConEx [CONEX]: a mechanism where senders inform the network about the congestion encountered by previous packets on the same flow, in-band at the IP layer.

- Latency versus Bandwith: allowing the content provider to indicate whether a better bandwidth or lower latency is of greater priority and allowing the network to react. Where this bit resides and how to authenticate it would need to be decided.

- No network management tools: disabling all network management tools from the network and allow the protocols to manage congestion alone.

- FlowQueue Codel [FLOWQUEUE]: a hybrid packet scheduler/AQM algorithm, aiming to reduce bufferbloat and latency. FQ-CoDel mixes packets from multiple flows and reduces the impact of head of line blocking from bursty traffic.

Many of these suggestions could be labeled "Network-to-App", a better approach may be "Network-to-User", to achieve this these ideas would need to be expanded. Others aim to create "hop-to-hop" solutions, which could be more inline with how congestion is managed today, but with greater privacy implications.

"App-to-Network" style solutions have either existed for a long time by implicit solutions, or explicitly defined but never implemented or properly deployed. Some workshop attendees agreed that applications

declaring was quality of service they require was not a good route given the lack of success in the past.

3.1.1. Trust and the Mobile Network Complexities

One of the larger issues in the sharing of data is the matter of trust; networks operators find difficulties in relinquishing data for reasons such as revealing competitive information and applications wish to protect their users and only reveal little information to the network. Authentication in that case could be a key design element of any new work, as well as explictness rather than the transparent middleboxes used more recently. Some workshop attendees suggested any exchange of information should be biodirectional, in an effort to improve trust between the elements. A robust incentive framework could provide a solution to the trust issue, or at least help mitigate it.

The radio access network is complex and manages a number of realities. Base stations understand many of these realities, and information within these base stations can be of value other entities on the path. Solutions for managing congestion on radio networks should involve the base station if possible. For instance, understanding how the Radio Resource Controller and AQM [RFC7567] interact (or don't interact) could provide valuable information for solving issues. Although many workshop attendees agreed that even though there is a need to understand the base station not all agreed that the base station should be part of a future solution.

Some suggested solutions were based on network categorisation and providing this information to the protocols or endpoints. Categorising radio networks could be impossible due to their complexity, but categorising essential network properties could be possible and valuable.

4. Transport Layer: Issues, Optimisation and Solutions

TCP has been the dominant transport protocol since TCP/IP replaced NCP on the Arpanet in March 1983. TCP was originally devised to work on a specific network model that did not anticipate the high error rates and highly variable available bandwidth scenarios experienced on modern radio access networks. Furthermore new network elements have been introduced (NATs and network devices with large buffers creating bufferbloat), and considerable peer-to-peer traffic is competing with traditional client-server traffic. Consequently the transport layer today has requirements beyond what TCP was designed to meet. TCP has other issues as well; too many services rely on TCP and only TCP, blocking deployment of new transport protocols like SCTP and DCCP. This means that true innovation on the transport

layer becomes difficult because deployment issues are more complicated than just building a new protocol.

The IETF is trying to solve these issues through the "Stack Evolution" programme, and the first step in this programme is to collect data. Network and content providers can provide data including: the cost of encryption, the advantages of network management tools, the deployment of protocols, and the effects when network management tools are disabled. Network operators do not tend to reveal network information mostly for competition reasons and so is unlikely to donate this information freely to IETF. The GSMA is in the position to collect this data and anonymise it before bringing it to IETF which should alleviate the network operator worries but still provide IETF with some usable data.

A considerable amount of work has already been done on TCP, especially innovation in bandwidth management and congestion control; although congestion is usually detected by detecting loss, and better methods based on detecting congestion would be beneficial.

Furthemore, although the deficiencies of TCP are often considered as key issues in the evolution of the stack, the main route to resolve these issues may not be a new TCP, but an evolved stack. SPUD [SPUD] and ICN [RFC7476] are two suggestions which may help here. QUIC [QUIC] engineers stated that the problems solves by QUIC are general problems, rather than TCP issues. This view was not shared by all attendees of the workshop. Moreover, TCP has had some improvements in the last few years which may mean some of the network lower layers should be investigated to see whether improvements can be made here.

5. Application Layer Optimisation, Caching and CDNs

Many discussions on the effects of encrypted traffic on radio access networks happen between implementers and the network operators; this session aimed to gather the opinions of the content and caching providers including their experiences running over mobile networks, the experience their users expect, and what they would like to achieve by working with or using the mobile network.

Content providers explained how even though this workshop cited encrypted data over radio access networks as the main issue the real issue is network management generally, and all actors (applications providers, networks and devices) need to work together to overcome theese general network management issues. Content providers explained how they assume the mobile networks are standard compliant. When the network is not standards compliant (e.g. using non standards compliant intermediaries) content providers can experience real costs

as users contact their support centres to report issues which are difficult to test for and build upon.

Content providers cited other common issues concerning data traffic over mobile networks. Data caps cause issues for users; users are confused about how data caps work or are unsure how expensive media is and how much data it consumes. DNS and DNS caching cause unpredictable results. Developers build products on networks not indicative of the networks their customers are using and not every organisation has the finances to build a caching infrastructure.

Strongly related to content providers, CDNs are understood to be a trusted deliver of content and have shown great success in fixed networks. Now traffic is moving more to mobile networks there is a need to place caches at the edge of the network (e.g. in the Gi LAN or the radio network) within the mobile network. Places caches at the edge of the mobile network is a solution, but requires standards developed by content providers and mobile network operators. The CNDi Working Group [CDNI] at IETF aims to allow global CDNs to interoperate with mobile CDNs; but this causes huge trust issues for the caching of encrypted data between these CDNs. Some CDNs are experimenting with "Keyless SSL" to enable safer storage of content without passing private keys to the CDN. Blind Caching is another proposal aimed at caching encrypted content closer to the user and managing the authentication at the original content provider servers.

At the end of the session the panelists were asked to identify one key collaborative work item, these were: evolving caching to cache encrypted content, uing one-bit for latency / bandwidth trade-off (explained below), better collaboration between the network and application, better metrics to aid bug solving and innovation, and indications from the network to allow the application to adapt.

6. Technical Analysis and Response to Potential Regulatory Reaction

This session was conducted under Chatham House Rule. The session aimed to discuss regulatory and politcal issues; but not their worth or need, rather to understand the laws that exist and how technologists can properly respond to these.

Mobile networks are regulated, compliance is mandatory (and can result in service license revocation in some nations round the world) and can incur costs on the mobile network operator. Regulation does vary geographically. Some regulations are court orders, others are "block lists" of websites such as the Internet Watch Foundation list [IWF]. Operators are not expected to decrypt sites, so those identified sites which are encrypted will not be blocked.

Parental control-type filters also exist on the network and are easily bypassed today, vastly limiting their effectiveness. Better solutions would allow for users to easily set these restirctions themselves. Other regulations are also hard to meet - such as user data patterns, or will become harder to collect - such as IoT cases. Most attendees agreed that if the governments cannot get the information from network operators they will approach the content providers. Some governments are aware of the impact of encryption and are working with or trying to work with content providers. The IAB have concluded blocking and filtering can be done at the endpoint of the communication.

These regulations do not always apply to the internet, and the internet community is not always aware of their existance. Collectively the internet community can work with GSMA and 3GPP and act collectively to alleviate the risk imposed by encrypted traffic for lawful intercept. The suggestion from attendees was that if any new technical solutions built should have the ability to be easily switched off.

Some mobile network operators are producing transparency reports covering regulations including lawful intercept. Operators who have done this already are encouraging others to do the same.

7. Requirements and Suggestions for Future Solutions

Based on the talks and discussions throughout the workshop a set of requirements and suggested solutions has been collected. This is not an exhaustve list.

- Encrypted Traffic: any solution should encourage and support encrypted traffic.

- Flexibility: radio access network qualities vary vastly and different network needs in content can be identified, so any new solution should be flexible to either the network type or content type or both.

- Privacy: new solutions should not introduce ways where information can be discovered flows and attribute them to users.

- Minimum data only for collaborative work: user data, app data and network data all needs protecting, so new solutions should use the minimum information to make a working solution.

A collection of solutions suggested throughout the workshop is given below. These solutions haven't been matched to the requirements above, so this step will need to come later.

- Evolving TCP or evolution on the transport layer: this could take a number of forms and some of this work is already existing within IETF. Other suggestions include:

- Congestion Control: many attendees cited congestion control as a key issue, further analysis, investigation and work could be done here.

- SPROUT: research at MIT which is a transport protocol for interactive applications that desire high throughput and low delay. [SPROUT]

- PCC: Performance-oriented Congestion Control: is a new architecture that aims for consistent high performance even in challenging scenarios. PCC enpoints observe the connection between their actions and their known performance, which allows them to adapt their actions. [PCC]

- CDNs and Caches: placing caches closer to the mobile user or making more intelligent CDNs would result in faster content delivery and less train on the network. Related work includes:

- Blind Caching: a proposal for caching of encrypted content [BLIND_CACHING].

- CDN improvements: including keyless SSL and better CDN placement.

- Mobile Throughput Guidance: a mechanism and protocol elements that allow the cellular network to provide near real-time information on capacity available to the TCP server. [MTG]

- One bit for latency / bandwidth tradeoff: using one bit to identify whether a stream prefers low latency at the expense of throughput. This rids solutions of the trust issue as applications will need to select the best scenario for their traffic type.

- Base Station: some suggestions involved "using the Base Station", but this was not defined in detail. The Base Station holds the Radio Resource Controller and scheduler which could provide either a place to host solutions or data from the Base Station could help in devising new solutions.

- Identify traffic types via 5-tuple: information from the 5-tuple could provide understanding of the traffic type which network management could then be applied.

- Heuristics: Networks can sometimes identify traffic types through specifics such as data flow rate and then apply network management to these identified flows. This is not recommended as categorisations can be incorrect.

- APIs: An API for operators to share congestion status or the state of a cell before an application starts sending data could allow applications to change their behaviour. Alternatively an API could provide the network with some information on the data type to provide network management to, although this method exposes privacy issues.

- Standard approach for operator to offer services to Content Providers: mobile network operators could provide caching services or other services for content providers to use for faster and smoother content delivery.

- AQM [AQM] and ECN [RFC3168] deployments: queueing and congestion management methods have existed for sometime in the form of AQM, ECN and others which can help the transport and internet layer adapt to congestion faster.

- Trust Model or Trust Framework: some solutions in this area (e.g. SPUD) have a reliance on trust when content providers or the network are being asked to add classifiers to their traffic.

- Keyless SSL: allows content providers to maintain their private keys on a "key server" and host the content elsewhere (e.g. on a CDN). This could become standardised in IETF. [LURK]

- Meaningful capacity sharing: including the ConEx [CONEX] work which exposes information about congestion to the network nodes.

- Hop-by-hop: some suggestions offer hop-by-hop methods allowing nodes to adapt flow given the qualities of the networks around them and the congestion they are experiencing.

- Metrics and metric standards: in order to evolve current protocols to be best suited to today's networks data is needed on the current network situations, protocol deployments, packet traces and middlebox behaviour. Futher than this proper testing and debugging on networks could provide great insight for stack evolution.

- 5G: Mobile operator standards bodies are in the process of setting the requirements for 5G, requirements for network management could be added.

In the workshop attendees identified other areas where greater understand could help the standards process. These were identified as:

- Greater understanding of the RAN at IETF
- Reviews and comments on 3GPP perspective
- How to do congestion controlling in RAN.

7.1. Better Collaboration

Throughout the workshop attendees placed emphasis on the need for better collaboration between the IETF and telecommunications bodies and organisations. The workshop was one such way to achieve this, but the good work and relationships built in the workshop should continue so the two groups can work on solutions which are better for both technologies and users.

8. Next Steps

The next steps for MaRNEW attendees are to begin work on a select list of the above recommended solutions and other suggestions within the IETF and within other organisations. At IETF95 the ACCORD BoF will be held which will bring the workshop discussion to the wider IETF attendance and select key areas to progress on; these are likely to be definitions of the metrics to be collected, more information on the stack evolution ideas and their impact to network management, Mobile Throughput Guidance evolution, evolution of the Blind Caching work and draft definitions of the "1 bit for latency / bandwidth tradeoff" idea. As identified in the "Better Collaboration" section together we need to ensure that both groups continue the positive relationship to move these ideas forward into being real and workable solutions and both groups need to understand that even though collaboration between the operator network and the internet is of great importance the item of most importance is the experience and security for the users using these services.

9. Informative References

[RFC7567] Baker, F., Ed. and G. Fairhurst, Ed., "IETF Recommendations Regarding Active Queue Management", BCP 197, RFC 7567, DOI 10.17487/RFC7567, July 2015, <http://www.rfc-editor.org/info/rfc7567>.

[RFC7476] Pentikousis, K., Ed., Ohlman, B., Corujo, D., Boggia, G., Tyson, G., Davies, E., Molinaro, A., and S. Eum, "Information-Centric Networking: Baseline Scenarios", RFC 7476, DOI 10.17487/RFC7476, March 2015, <http://www.rfc-editor.org/info/rfc7476>.

[RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, DOI 10.17487/RFC3168, September 2001, <http://www.rfc-editor.org/info/rfc3168>.

[NOTE_WELL] "IETF Note Well", n.d., <https://www.ietf.org/about/note-well.html>.

[MARNEW] "MaRNEW Workshop IAB Homepage", n.d., <https://www.iab.org/activities/workshops/marnew/>.

[CHATHAM_HOUSE_RULE] "Chatham House Rule", n.d., <https://www.chathamhouse.org/about/chatham-house-rule>.

[GSMA] "GSMA Homepage", n.d., <http://gsma.com>.

[SDO_3GPP] "3GPP Homepage", n.d., <http://www.3gpp.org/>.

[PCC-QOS] "Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping", March 2016, <http://www.3gpp.org/DynaReport/29213.htm>.

[STATE_BROWSER] Barnes, R., "Some observations of TLS in the web", July 2015, <https://www.ietf.org/proceedings/93/slides/slides-93-saag-3.pdf>.

[STATE_SERVER] Salz, R., "Some observations of TLS in the web", July 2015, <https://www.ietf.org/proceedings/93/slides/slides-93-saag-4.pdf>.

[TCPINC] "TCP Increased Security Working Group", n.d., <https://datatracker.ietf.org/wg/tcpinc/charter/>.

[UBIQUITOUS] Morton, K., "Effect of Ubiquitous Encryption", March 2015, <https://tools.ietf.org/html/draft-mm-wg-effect-encrypt-01>.

[NETWORK_MANAGEMENT]
Smith, K., "Network management of encrypted traffic", May 2015, <https://tools.ietf.org/html/draft-smith-encrypted-traffic-management-00>.

[Pew2014] "Public Perceptions of Privacy and Security in the Post-Snowden Era", November 2014, <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>.

[MTG] Smith, A., "Mobile Throughput Guidance Inband Signaling Protocol", September 2015, <https://www.ietf.org/archive/id/draft-flinck-mobile-throughput-guidance-03.txt>.

[SPUD] "Session Protocol for User Datagrams", n.d., <https://datatracker.ietf.org/wg/spud/documents/>.

[CONEX] "Congestion Exposure Working Group", n.d., <https://datatracker.ietf.org/wg/conex/documents/>.

[FLOWQUEUE]
Dumazet, P., "FlowQueue-Codel", March 2014, <https://tools.ietf.org/html/draft-hoeiland-joergensen-aqm-fq-codel-00>.

[QUIC] Swett, J., "QUIC, A UDP-Based Secure and Reliable Transport for HTTP/2", June 2015, <https://tools.ietf.org/html/draft-tsvwg-quic-protocol-00>.

[CDNI] "Content Delivery Networks Interconnection Working Group", n.d., <https://datatracker.ietf.org/wg/cdni/charter/>.

[IWF] "Internet Watch Foundation", n.d., <https://www.iwf.org.uk/>.

[SPROUT] Balakrishnan, K., "Stochastic Forecasts Achieve High Throughput and Low Delay over Cellular Networks", April 2013, <https://www.usenix.org/system/files/conference/nsdi13/nsdi13-final113.pdf>.

[PCC] Schapira, M., "PCC, Re-architecting Congestion Control for Consistent High Performance", May 2015, <http://arxiv.org/pdf/1409.7092v3.pdf>.

[BLIND_CACHING]
Holmberg, M., "An Architecture for Secure Content Delegation using HTTP", n.d., <https://tools.ietf.org/html/draft-thomson-http-scd-00>.

[LURK] Ma, D., "TLS/DTLS Content Provider Edge Server Split Use Case", January 2016, <https://tools.ietf.org/html/draft-mglt-lurk-tls-use-cases-00>.

Author's Address

Natasha Rooney
GSMA

Email: nrooney@gsma.com
URI: https://gsma.com