

Spread Spectrum Voice over IP

E P Wentworth, Department of Computer Science, Rhodes University, Grahamstown, South Africa
p.wentworth@ru.ac.za; phone +27-46-603-8291; fax+27-46-636-1915

Abstract—ISPs and Internet users locate the intelligence outside of the network, and prefer to see the essential and key role of the network as just carrying the bits. Telecommunications providers need to build intelligence into the core of the network so that the network remains aware of the high-value services and can be a meaningful part of the revenue stream. The intelligence is also regarded as a key tool which will help the operators classify traffic flows, and understand their nature, so that the operators can act to prevent their high-value services from being bypassed on their own cheaper IP or bandwidth pipes.

Proposed traffic identification mechanisms include deep packet inspection – and statistical profile analyses on flows of packets, to enable the network to recognize, for example, VoIP traffic.

Deep packet inspection is easily foiled with encryption and tunneling workarounds. The paper also proposes a simple new mechanism for foiling statistical detection, based on frequency-hopping spread-spectrum principles.

The author predicts the emergence of a cat-and-mouse game with regulatory, marketing and technical offensive and defensive moves to protect or claim territory. The mechanisms discussed here are the opening gambits.

Index Terms—Deep Packet Inspection, Spread Spectrum, Revenue Bypass, Statistical Profiling, VoIP

I. INTRODUCTION

In 1997, David S. Isenberg, a former AT&T researcher, wrote a seminal paper titled *The Rise of the Stupid Network*[1]. A stupid network is one whose sole function is to “just deliver the bits”. In a stupid network, the intelligence, session control, congestion control, protocol negotiation, gateway translation functions, and billing all reside in the intelligent end-points, be they servers or clients. Our biggest truly stupid network, the Internet, has proved resilient, remarkably adaptable, and hugely successful. Google was started in 1998, and is now worth considerably more than BT, with a lineage going back to 1846.

The problem is that stupid networks disintermediate the incumbent telecommunications operators (telcos) from the high value-add activities in the value chain. Services in the Internet are created, supplied and operated from intelligence residing outside the edge of the telcos’ networks. Activities like shopping, searching, processing credit card transactions, and Internet banking bring no new revenue to the telcos, other than the sliver of revenue for carrying the bits.

Not earning new revenue from new markets is perhaps tolerable. But the new tide of low-cost IP-based services that erodes (or threatens) established telco revenue streams is forcing them to make countermoves. Voice over IP (VoIP) is

threatening voice revenues, instant messaging could erode SMS, e-mails are displacing faxes, VoIP over GPRS threatens GSM voice revenues, and commoditized Virtual Private Network (VPN) endpoints allow users to self-provide VPNs over Internet instead of leasing tie lines..

In his keynote address[2] to the International Engineering Consortium, Rod Randall, a former Chief Marketing Officer of Lucent Technologies, presents a common theme. The network needs intelligence rather than stupidity, so that it can understand the traffic it carries, and be an integral part of the value chain. When the user watches a movie, some slice of the value-added rental fee should be collectible by the telcos. By understanding, policing, and censoring the flows of traffic, the operators should and can build fences between high and low value traffic, prevent the migration of high-value services onto low-value pipes, and ensure that they play a meaningful role in the high revenue services that use their infrastructure.

So does one put the intelligence in the network, or outside? The Netheads¹ favour a stupid network with the intelligence and control in their own hands. The Bellheads need intelligence, control and management inside the network in order to make workable business cases. While Bellheads build intelligence into the core, Netheads will be leasing more raw bandwidth more cheaply to overlay their stupid network. In their simplistic model, more bandwidth over time automatically brings improved quality.

We predict the emergence of a cat-and-mouse game.. The Bellheads will make a move to detect, block, and prevent activity that threatens them, and the Netheads will respond by seeking workarounds. This battle will have regulatory, marketing and technological dimensions.

II. BYPASS

Not all bits in the network are of equal value to Telecommunications operators. The earnings-per-bit for SMS or voice calls are orders of magnitude more than the earnings-per-bit for bulk data services over the Internet. This creates entrepreneurial opportunities for *bypass* applications to redirect high-value traffic onto cheaper bearer channels.

Adoption is slowed by quality and other considerations, but for most disruptive technologies[4] the quality of the new offering improves over time to overtake the users requirements[4, pg xix], so eventually dominates.

Voice over IP (VoIP), Least Cost Routing, voice calls

¹ Following [3], we call the opposing camps the *Netheads*, (the ISPs and Internet users raised and cultured in the ways of the packet-based Internet), and the *Bellheads*, (those who have inherited their philosophy and culture from the circuit-dominated networks of Bell and AT&T).

over GPRS rather than GSM, and Virtual Private Networks over the Internet are all examples of bypass schemes which initially offer lower quality, no committed bit rate, more dropped packets, and fewer successful end-to-end call setups. But quality on all these is rapidly improving.

III. DEEP PACKET INSPECTION, AND COUNTERMEASURES

One proposed countermeasure to bypass is to build intelligence into the network to perform *deep packet inspection* – to examine the destination ports, contents, and protocols detect “improper” use of the network, and to classify traffic for differential billing purposes.

In TCP/IP networks, the port identifies a particular application within a host machine on the Internet. For example, port 80 usually denotes a web service. But the associations are by convention only, and end-points could agree to use different ports to bypass a port inspector.

Deep inspection into the contents of the packets is also easily preventable with end-to-end encryption, an essential part of every secure browsing session with your bank.

Traffic identification by protocol type is equally ineffective. A *tunnel* allows one to take any kind of traffic and “rewrap” it in a different protocol packaging for the purposes of transport, allowing one to “smuggle” any kind of traffic through the Internet disguised as other traffic.

Encrypted tunnels are used extensively for VPNs, so a VPN end-to-end connection will defeat all three of the inspection tests mentioned here.

IV. STATISTICAL PROFILING, AND COUNTERMEASURES

More recent proposals are to perform statistical profile analyses on flows of packets, to enable the network to classify or recognize VoIP traffic. We propose a simple mechanism for foiling statistical detection, based on frequency-hopping spread-spectrum principles.

Frequency hopping, originally co-invented by the glamorous Hollywood actress Hedy Lamarr in 1940[5], was designed to prevent the enemy from intercepting and jamming radio frequency guidance mechanisms on torpedoes. By rapidly hopping wireless transmission frequencies in a secret *spreading code* pattern, known only to the aggressor, two objectives are achieved: the mere presence of the guidance channel becomes virtually undetectable against the background noise, and even if the enemy can see the torpedo approaching, they cannot lock on to the pattern to disrupt it.

Hiding the statistical nature of an VoIP channel simply becomes a matter of doing what was already well understood in the 1940s – we establish an array of independent channels (TCP/UDP/RTP connections) between the endpoints, and spread the data between them using a privately agreed spreading code. The data is reassembled on the other side. We dub this *Spread Spectrum Voice over IP*. The technique is also applicable to any other flow-based IP service.

We could perhaps use more than one network to carry the underlying traffic – some of the packets can flow through the GPRS network, and others split between services from multiple network operators.

Splitting a TCP flow into many smaller flows may incur

performance penalties. (Although VoIP is unlikely to use “reliable” TCP transports, other bypass systems might.) Recent studies have highlighted correlations between different packet flows that traverse the same underlying physical network node at some point of congestion[6]. In particular with TCP, since each flow in the network makes its own uncoordinated congestion avoidance decisions, the flows can interfere with each other and lead to globally sub-optimal performance. In this literature, the suggestion is to improve performance by aggregating flows into one TCP stream which will not compete with itself.

Aggregation of flows, rather than splitting flows suggests yet another avenue for bypassing statistical detection of traffic types. An organization with N active sessions that are bypassing an expensive channel could aggregate the data into a single transport stream whose statistical profile would differ considerably from what the inspector was looking for.

V. CONCLUSION

The rise of a stupid network with the decision-making and intelligence in the hands of the users will continue to attract Netheads who will create bypass mechanisms and migrate all traffic to the cheapest bandwidth pipes. Increased intelligence in the network will continue to be attract Bellheads who need to prevent their high-value services from being bypassed on their own infrastructure. Deep packet inspection and statistical profiling are just two current technical proposals for identifying bypass traffic. Each has fairly trivial workarounds.

REFERENCES

- [1] David S. Isenberg, *The Rise of the Stupid Network*. Follow the link from <http://www.isen.com/>
- [2] Roderick Randall, *The Future of Network Intelligence*, keynote address at 21st Century Communications WorldForum conference, 2005, available at http://www.iec.org/online/iforums/iec_3/choose.asp
- [3] Steven G. Steinberg, *Netheads vs Bellheads*, www.wired.com/wired/archive/4.10/atm.html
- [4] Clayton M. Christensen, *The Innovators Dilemma*, HarperBusinessEssentials, 2003.
- [5] Answers.com *Spread Spectrum*, <http://www.answers.com/Spread%20spectrum>
- [6] Rubenstein, D., Kurose, J., Towsley, D., Detecting Shared Congestion Flows Via End-to-end Measurement, Technical Report 99-66, Department of Computer Science, University of Massachusetts, 1999, http://citeseer.ist.psu.edu/cache/papers/cs/14117/ftp:zSzzSzg_aia.cs.umass.edu/SzpubzSzRubenst99_SPOC-TR-99-66.pdf/rubenstein99detecting.pdf

Peter Wentworth is a Professor of Computer Science at Rhodes University, and co-founder and Director of 7 Fountains Digital (Pty) Ltd, an SMME providing IT and Telecommunication consulting, training, and specialist software for industry. His interests include IP networking, Telecommunications strategies, Metro-Ethernet, and Web Services.