TOWARD A POLYMORPHIC FUTURE INTERNET: A NETWORKING SCIENCE APPROACH

Kavé Salamatian,

LISTIC Lab
Université de Savoie
Annecy-le-Vieux, France

ABSTRACT

In this paper, I will develop two major claims. First the, Future Internet should be polymorphic and conciliate different architectural paradigms networking. The second claim is that the Future Internet should be build on strong theoretical basis from a Networking science that is in course of development.

In this paper, I have used the concept of cooperation as an interpretation lens. Specifically, I will describe how virtualisation make possible a polymorphic future Internet and enables the easy deployment of new cooperation schemes. The next aspect that I describe in this paper is relative to security in the future Internet. Particularly the paper advocates the necessity of three major components: a secure execution platform, an authentication mechanism, and a monitoring component. Finally, I will show that it is possible to build scalable addressing and routing scheme but at the condition of following a clean slate approach.

Index Terms— Future Internet, Internet Science, Network Architecture

1. INTRODUCTION

Based on one of the major stories about the origin of the Internet, Internet came to the age of 40 at 22:30 hours on October 29, 1969. During its 40 years lifetime, it grew from a small three nodes network build mainly for computer time-sharing, to a network connecting an estimated 1,800 million users and a penetration rate of almost 25%. No human built system has ever reached such a growth rate in such a short time. What was once a tool known and used by only a small intelligentsia of high profile researchers, has become within one generation a universal commodity, like electricity, in the daily life of hundreds of millions of users. This shed light on the importance of the on going discussion about the "future Internet." Several initiatives envision the definition, the design, and the construction of this future Internet. On the research side, the US based GENI (Global Environment for Network Innovation) initiative [1], and the European Union FIRE (Future Internet Research and Experimentation) initiative [2] are noteworthy and many of other activities in different countries can be cited. More generally, the United Nations World Summits on Information Society held in 2007 and 2009 enlarged the scope of Internet as the main component of the Information Society of the future by introducing cultural aspects in a more formal way. That said, this flurry of interest on the future of Internet is also a source of confusion; different and competitive requirements as well as architectural concepts are fogging our vision of the future of Internet.

My aim in this talk is indeed not to add up to the existing fog by sprinkling my "*yet another*" new and clever architectural conception of how the community should shape the future of the Internet. I have in this paper two claims: first that future Internet should be polymorphic, *i.e.* that it will need to conciliate inside it different architectural paradigms. Particularly, the future Internet would have (at least in a long transitory period) to support the evolution of the current Internet in form of IPv6 or any other evolution of the current IP architecture along with other more revolutionary paradigms. Therefore, the main property of the future Internet should be flexibility to enable their smooth coexistence. My second position is that networking is not simply a technological artefact, but it is becoming a separate science that borrows some of its principles from other well-established sciences as computer science, physics, social science, *etc.* and has also its own particular fundamental laws and principles, similar to any other science. Describing the particular principles of this "*Networking Science*" and differentiating them from the principles of other sciences is one of the major scientific challenges that the Internet and more generally the networking research community has to overcome in the coming years. Indeed, by looking at networking in its broadest view, one can see that networking in form of roads, postal service and telephony have a very long history. However, it is only during the past years that with the development of social networks and wide availability of Internet that it becomes obvious that these historical networks and the new comer Internet should have common principles that have still to be fully investigated in the context of networking science.

Obviously, if such networking fundamental principles exist, the future Internet will also follow them naturally. Unfortunately, finding fundamental principles for networks is still a research effort. Being realistic, I will only be able in this paper, to shed some lights about major questions that the community will have to tackle in the path toward the future Internet. Being invited to give a keynote, I will be a little

more radical than I am generally as I want to ignite thought-provoking discussions and open new perspectives.

2. COOPERATION: THE VERY ESSENCE OF NETWORKING

First, let's dig into the basics of networking. It is possible to define a network as a set of nodes that are cooperating with each other to distribute (exchange) information. However, one has to formalise the concept of cooperation further. The main role of a node in a network is to generate information in form of messages, packets, signals, *etc.* We can therefore state that a networking component receives from its neighbours (other components, nodes, or layers) and/or its environment a sequence of incoming messages or information and generates a sequence of outgoing messages. The relation between incoming and outgoing information streams defines the cooperation function (or forwarding function) the node implements.

We have been educated to consider networks through the layered approach of the Open Systems Interconnection (OSI) model. In this approach the inputs to the cooperation function come only from the predecessor layer and concern variables relative to components in the same layer; the resulting value is sent to next layer. Therefore, the layered architecture and the associated protocols constrains the space of possible cooperations between nodes to make it tractable and to formalise it. This layered view has been the major architectural paradigm in the past three decades. Layers opacity and independence enabled the programmers to concentrate on a single layer and to implement services without needing to tussle with other layers.

However, layering comes with a performance cost. Cross layering, *i.e.* enabling a layer to access information and to interact with any other layers, has been advocated for higher efficiency, performance, resource management, and security. These arguments have been important in the emergence of the "*autonomic network*" idea. In this approach, a network component is seen as an active element that is "*self-conscious*" and that interacts with its environment.

All the above considerations have resulted in a major shift of the networking paradigm that has moved away from a layered, to a puzzle view where autonomic components are "*co-operating*" with each other. This results in enabling the use of information coming from different layers for implementing the cooperation function. The classical view considered the operation of a network element as processing packets. Now the role of a network is considered as deciding (based on data received in the past and information's gathered from the environment) which type of cooperative functions the node (or the node owner) should be implemented to achieve the goals of the network (defined by the network operator, or the service provider), as well as its selfish goals (defined by the owner of the node). This opens the way for a node to behave differently from what the classical protocols predict (for example to go to a standby mode, or to open a tunnel to implements its specific cooperation function). Accepting that nodes can be selfish is a major change, motivated by applicative scenarios like ad-hoc wireless networks where one cannot assume that all nodes will belong to the same authority. Inter-domain routing at the Autonomous System (AS) level is another scenario where selfishness is essential. In this last situation, the different network operators have to cooperate even if they might be in fierce competition. Cooperation between selfish nodes is a central element of the future Internet architecture.

Moreover, cooperation is also the central concept of this developing science of networking. Networking science studies the production, distribution, and consumption of "information" and is cooperation for information exchange, precisely what a network does! Information has some specific properties that differentiate it from other goods and therefore necessitate a new theoretical treatment: information is universal and infinitely reusable, *i.e.*, a bit of information can be duplicated and shared infinitely at almost no cost. Another difference is that information is ambiguous, *i.e.* you might receive ambiguous messages when other goods and services are unambiguous. These two peculiar properties that are the basis of Information Theory as developed by Shannon differentiate Networking science from Classical economy. To illustrate this difference, one can look at the controversy existing in the economical literature on the Efficient-Market Hypothesis that asserts that financial markets are "informationally efficient". This hypothesis assumes that prices on traded assets (e.g., stocks, bonds, or property) reflect all past available information. However, the validity of this hypothesis has been questioned (critics even blame the belief in rational markets for much of the financial crisis of 2007–2010). This shows that unconsciously information is seen as an external concept helping in shaping the prices, and not as a normal asset and some mechanisms should be provided to make this information available to make market efficient.

While, in the layered view, network services are built over a predefined set of cooperation primitives (named Service Access Points in the OSI jargon), in autonomic networks the node has to permanently monitor its environment to optimise its cooperative behaviour based on information coming from a different layer of the classical layered architecture. While the optimisation can result in better performance, it adds a level of complexity and careless optimisation can even lead to lower performance as the information coming from different level of networks can be contradictory. A major challenge facing the networking research community consists of developing methods for online and autonomic optimisation of this cooperation.

3. TO CLEAN THE SLATE OR NOT? IS IT REALLY AN ISSUE?

From its inception 40 years ago, Internet was designed, developed and deployed simultaneously. More precisely whenever a problem arose, a solution was proposed and analysed following a technical consensus at the IETF resulting in a Request For Comment (RFC) solving the issue or implementing

a new feature. The IETF consensus guaranted that the proposed evolution of Internet was backward compatible and was complying with the sacrosanct axiom of "no harm to what works". The previous guarantee is one of the explanation of the huge success and relative stability of current Internet. However, the drawback of this approach is that it contrains the future evolution and hinders the deployment of radical solutions that attack the problems at the source. This is one major reason for the clean slate approach advocated by a part of the community.

The clean slate approach comes from the belief that it is impossible to resolve the challenges facing today's Internet without rethinking the fundamental assumptions and design decisions underlying its current architecture. The incremental approach changes the Internet architecture by backward compatible patches; the clean slate approach advocates out of the box thinking with an architectural redesign with better concepts and abstractions to answer the current challenges.

However, as explained in the introduction we expect the future Internet to be polymorphic. Specifically the future Internet should be flexible enough to conciliate coexistence of the evolution of the actual Internet with the incremental patches with approaches coming out of the clean slate vision. Therefore, the future Internet should be designed so that the question of cleaning the slate or not should not be anymore relevant. Clean slate–based revolutionary research should go along with evolutionary approaches to ensure that the working Internet will still continue to work in parallel with new architecture with more features. We will describe later why we believe that such a flexibility is achievable and why therefore cleaning the slate or not is not an issue.

Nonetheless, imagining new architecture is a tough task. We need to choose among the large set of possible architectures, the few that could take the relay of the current Internet. For this purpose, we need to experiment different architectures in large scale experimental facilities. This explains why almost all initiative on the future Internet are backed by a large scale experimental facility like PlanetLab [3], GENI [1], *etc.*

4. A CRITICAL ANALYSIS OF THE FUTURE INTERNET MOTIVATIONS AND RATIONALES

It is natural to ask why people are questing for a future Internet. Internet as we know it today has certainly gone beyond the wildest expectations of it is first pioneers and even its current status addresses a large spectra of nowadays needs. However, there is a consensus in the research community and in larger audience that the current Internet has some shortages that make its evolution and/or revolution inevitable. I will give here some of the main reasons that are provided and shed some lights on the directions to go.

4.1. Flexibility or the future Internet contortionist

I explained previously that the future Internet should be polymorphic and its architecture be flexible enough to accommodate different cooperation paradigms in parallel. Another rationale for a flexible future Internet architecture is relative to new application deployment. The current Internet provides a very large freedom for developers to develop their own applicative protocols. However, it does not provide architectural hooks to deploy services beyond the socket interface; developers have no access to routing and addressing. But routing is an essential component for the cooperation provided by network. For this reason during the past decade, routing and addressing was frequently raised into the application level where the developers can have an impact on them.

Peer to Peer and overlay networks are examples of this approach and implement a complete cooperation scheme into the application level (more precisely above the socket interface). While this approach has been very successful, it is not really optimal as the packets have still to go through the underlying services narrow hip hourglass of IP that acts as a bottleneck. A network where one could implement, and deploy its new network protocols or cooperation schemes without disturbing other running protocols, would solve the application deployment issue, and will moreover provide a fantastic platform for innovative service deployment.

The quest for a flexible platform that will enable concurrent execution of different networking mechanisms along with easy deployment has been pursued in the networking research community with the objective of building a flexible experimentation platform for the future Internet research. This has resulted in the development of Planetlab [3], its European counterpart OneLab [4] and Global Environment for Network Innovations (GENI) [1]. The flexibility in these experimental platforms was attained thanks to the wide generalisation of virtualisation approaches [5] that enabled the parallel running of several virtual machines over a single hardware. As virtualisation ensures full isolation (fault, software, and performance isolation) between virtual machines, it enables the parallel execution of different networking systems (routing, addressing, *etc.*) and opens the way for the polymorphic future Internet I was advocating.

Virtualisation techniques also ensure the ability to encapsulate a full virtual machine into a single file that can be easily migrated to a virtualised hardware and being run on it. The encapsulation property opens the perspective of easy deployment of services by just distributing encapsulated virtual machine implementing the service over a large infrastructure of virtualised servers/routers. Last but not least, virtualisation approaches also ensure Interposition (to be discussed below) for monitoring and security. With the continuous increase in processing power available in commodity hardware, there has been a growing interest in developing new router architectures based on virtualisation running over clusters of multicore computers. This opens the perspective of building realistic routers implementing the polymorphic future Internet.

4.2. Security: the Achille's heel of the current Internet

One of the major rationales for the development of a future Internet is security. Indeed, the current Internet is plagued

with spam, phishing, denial of service attacks, exploits and other security problems. However, one should be careful to not mix apples and oranges. Only a small proportion of problems referred as related to security, are resulting from the Internet architecture, *e.g.*, even if phishing is an important security issue, it cannot be related directly to Internet architecture. One has therefore, to separate what is relative to application security (ensuring that an application is doing what it is supposed to do), to communication security (ensuring that communication remain secret) and finally to network security (ensuring that cooperation on network is secure).

The approach of the current Internet architecture to security is minimalist. Security was not considered to be an essential component of the network architecture, even in IPv6 that integrates an IPSEC component. It was seen at best as an optional service. The absence of security-related elements inside the architecture can be seen as the root cause of the current security status, where we have an abundance of security service (VPNs, firewalls, proxies, SSL, *etc.*). As a reaction, some advocate for integrating all security primitives inside the architecture so that application can fully rely on network security services. This last view is also highly questionable as too much security has a heavy impact on network devices performance. The future Internet will have to find an in–between way between these two extremes. Indeed, the future Internet architecture should provide some support for application and communication security. However, we have still to determine the least common denominator of security support that should be integrated into the architecture and what should be seen rather as a service that will cooperate with other components through the architecture.

It is noteworthy that security is a negative concept: you do not know when you have it; you only know when you have lost it. This means that, rather than speak about providing security, one should talk about reducing the vulnerabilities. Almost 30 years of experience in Internet security has taught us that it is impossible (and too costly) to remove all risks, meaning that we have to accept that we will continue to live with a risky network. The consequence of the above statement in cooperation terms is that we have to increase the resilience of the future Internet architecture to ensure survivability and to reduce the impact of security risks. In other words, security risks should be assumed as plausible operational hypothesis in the design of networked system and architectural solution should be provided to detect and to contain them. This is a radically different position from the current approaches where the emphasis is rather put on authentication of users through passwords/biometrics and assuming that authenticated users are entitled to do whatever they do. In the collaborative approach, we have to assume that users (even authenticated) can misbehave and we should be able to detect and contain them.

Therefore, in the light of cooperation concerns, the future Internet architecture needs at least three basic security mechanisms: a mechanism shielding strictly and at the deepest level possible components running in the same execution environment (like a sandbox), a mechanism ensuring authentication (the type and level of authentication still pending) to ensure the identity of the running code owner, and a monitoring mechanism that will evaluate the cooperation behaviour of executing components and compare them with some normal or expected behaviours. None of these mechanisms exist nowadays in Internet, but the current proposal of building the future Internet with virtualised concepts goes in the direction of addressing the first and last needs, as system virtualisation should guarantee fault, performance, and execution isolation, and monitor (or hypervisor or virtual machine monitor) interposition. It is, however, noteworthy that even if we have now monitoring mechanisms in virtualisation kernels, very little is known on the methodology of monitoring to detect abnormalities of networking components. The authentication service is also still subject to discussion. It is not yet clear if a global authentication and/or identity mechanism is mandatory, or only a local, and trust-based scheme will be enough to cover the large spectrum of scenario the future Internet will have to deal with.

The necessity of monitoring results is a major tradeoff between performance and security; the more security we choose, the stricter and the more exhaustive would be the monitoring. This results in a higher share of processing power assigned to monitoring and therefore a loss of performance for the monitored activities. Moreover, monitoring means also to reduce the range of acceptable behaviour to be able to differentiate them from abnormal ones. We have also a tradeoff between flexibility (in term of the range of acceptable behaviour) and security. So, while security nowadays is an important issue in Internet, it seems that security for the future Internet should be considered with a paradigm shift rather than just trying to push existing approaches and mechanisms into the foundations of the new architecture.

4.3. Scalability or the delusion of grandeurs

Another issue that should be considered in the future Internet is scalability. The past decade has seen a mean growth of Internet traffic of almost 100% per year. The size of routing table that is the main indicator of the complexity of the routing operation has seen a yearly growth of 19.4% from 2002 to 2008 [6]. Even if this rate has decreased to 8% during the past two years because of exhaustion of IPv4 address space (that is expected to happen in mid 2011) the growth rate is still considerable. Moreover, mobile Internet revolution and the Internet of things will increase significantly the dimension of the devices connected trough Internet space.

The current Internet has dealt with scalability by using a hierarchical architecture separating the different issues of routing in three different levels. The lowest level deals with local connectivity and configuration of interfaces IP addresses link layer mechanisms (essentially through Ethernet). The second level introduces IP routing between subnets by assuming that the local connectivity is provided inside a network mask. The third level implements operators' policies through BGP filtering and announcement rules, assuming that an AS operator is wise enough to provide optimal connectivity inside

itself.

Once upon a time, not so far in 1981, one could read in RFC 790, "*The assignment of numbers is also handled by Jon. If you are developing a protocol or application that will require the use of a link, socket, port, protocol, or network number please contact Jon to receive a number assignment*." Indeed, this situation was not tenable and Regional Internet Registries (RIR) took care of Internet addresses. However, address allocations had to remain compatible with previously allocated addresses. This backward compatibility constraint results in address fragmentation. CIDR (Classless Internet Domain Routing) was an attempt to reduce the burden of the past allocations. Indeed, this leveraged the pressure of address space exhaustion, but it did not solve radically the problem. The IPv6 standard solved radically the issue of address space exhaustion, and gave the impression that with an almost unlimited addressing space, its optimisation is not anymore needed. However, even with IPv6 the source of the scalability problem that was address space fragmentation remained. Moreover, IPv6 showed the difficulty of introducing radical changes into the network. Nearly a decade after most of the IPv6 standard was completed the vast majority of software and hardware still uses IPv4.

IPv6 never answered the cardinal question: "why do we need an address and how can we answer this need?" A trivial answer can be: "We need addresses to do routing." This lead to an even more radical question: "do we need routing?" The advent of Delay Tolerant Networks showed that routing might not be possible in some scenarios. It was even shown that network coding, which is not based on routing, is the forwarding scheme optimising the throughput [7]. More precise investigation shows that IPv6 or IPv4, rather than providing an answer for addressing needs, provides a roughly clever way of indexing the 32 or 128 bits address space. The past decade has seen first attempts at answering the general question of addressing. In these works, addressing was defined as a topological embedding adapted to a particular cooperation need, *i.e.* addressing is a function returning the position of the needed information into a topological space. It was shown that when the embedding is compact, *i.e.* when two close-by items are mapped by the addressing embedding into close addresses, addressing implies routing and *vice–versa*. In other words, if one knows the address of what he wants, he can derive directly from the address the path to reach it. This property means that scalable routing is possible and even trivial, when a compact embedding exists. Indeed, IP (either v4 or v6) addressing is not compact as close nodes are not necessarily close in the IP address space. Nonetheless, compact embeddings exist. For example, Content Addressable Network (with the assumption of no node withdrawal) [8] defines a compact embedding. The question of knowing whether we can embed the particular addressing need of a specific cooperation scheme into a compact embedding is one of the major questions of the Networking Science. For example, very general embeddings can be build that maps an IP like address space into a compact space with some performance costs [9]. Peer–to–Peer (P2P) and overlay networks have demonstrated that by lifting IP addressing backward compatibility constrainsts, scalability can be achieved and address fragmentation avoided. This validates the necessity of having a clean-slate approach rather than an evolutionary approach for developing the future Internet to enable deployment of new addressing/routing schemes. Indeed, one can note that IP addresses is still needed even on P2P or overlay networks. However, this is more a kind of link layer connectivity issue than a fundamental need of IP addressing.

This discussion sheds light on how to ensure the scalability of routing and addressing in future Internet. To summarize, contrary to the current Internet where routing tables are populated only with non-compact IP addresses, the future Internet should enable more flexible routing schemes with the choice of the suitable addressing embedding. Anyway, as explained before, the future Internet would be polymorphic and should simultaneously support execution of different addressing/routing schemes (embeddings), so that classical IPv4/v6 routing and addressing is expected to co-exist with more scalable schemes.

5. CONCLUSION

In this paper, we stated two main positions. First that the future Internet should be polymorphic, meaning that it should enable the coexistence of different networking paradigms in the same framework. I advocated that virtualisation techniques that are nowadays common provide the flexible technology needed for building such a polymorphic future Internet. The second position in this paper is that the future Internet needs a networking science to build strongly its foundations over it. I stated that the essential concept in the scientific approach to network is the concept of cooperation, and I used this concept to analyse some of the important issues I foresee for the future Internet design and deployment. This discussion resulted in some views on security, scalability, and flexibility in the current and the future Internet.

Specifically, I argued that the future Internet would be polymorphic. So the future Internet architecture should take advantage from the flexibility resulting from virtualisation to make possible a polymorphic architecture that adapts to the specific cooperation needs of the network applications. This flexibility will also be mandatory to ensure that new applications and services can be easily deployed in the future Internet, making this platform more attractive than the current Internet for innovation and businesses. The next aspect discussed in the paper was security. My position about security was that the future Internet will need to integrate some security mechanisms in its core architecture. I listed three basic and mandatory mechanisms: a secure execution platform (that could be provided by sandbox virtualisation), an authentication mechanism with an identification scope that has yet to be defined, and a monitoring component that could observe networking (cooperation) activity and eventually filter out all anomalous activities. The last topic developed in the paper was scalability. My position is that recent theoretical

works showed that it is possible to construct infinitely scalable addressing and routing scheme by using suitable embeddings. This adds some arguments, to other strong rationales, in favor of a clean slate approach to future Internet design where out-of-the-box thinking with an architectural redesign is possible. Nonetheless, I argued that if future Internet is designed with polymorphism in mind, to clean the slate or not is not anymore a crucial question, as the future Internet should be able to accommodate a completely revolutionary networking architecture as well as a more evolutionary one.

At the end, I would like to thank Serge Fdida, Professor at Paris VI university about interesting discussions about the architecture of Future Internet, and the anonymous reviewers for their valuable advice.

6. REFERENCES

[1] Chip Elliott and Aaron Falk, "An update on the geni project," *SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 3, pp. 28–34, 2009.

[2] Anastasius Gavras, Arto Karila, Serge Fdida, and Martin Potts, "M.potts. future internet research and experimentation," *The FIRE Initiative. ACM Computer Communication Review (CCR*, 2007.

[3] Larry Paterson and Timothy Roscoe, "The Design Principles of PlanetLab," *Operating Systems Review*, vol. 40, no. 1, pp. 11–16, January 2006.

[4] Ignacio Soto, Antonio de la Oliva, Bennoit Donnet, and Thierry Parmentelat, "A multi-homing architecture for onelab," *Paper presented at Real Overlays And Distributed Systems (ROADS) Workshop. (Warsaw, Poland)*, July 2007.

[5] Thomas Anderson, Larry Peterson, Scott Shenker, and Jonathan Turner, "Overcoming the internet impasse through virtualization," *Computer*, vol. 38, no. 4, pp. 34–41, 2005.

[6] G. Huston, "BGP table size," accessed 2010-10-11 online at http://bgp.potaroo.net/index-bgp.html.

[7] Junning Liu, Dennis Goeckel, and Don Towsley, "Bounds on the throughput gain of network coding in unicast and multicast wireless networks," *IEEE J.Sel. A. Commun.*, vol. 27, no. 5, pp. 582–592, 2009.

[8] Sylvia Ratnasamy, Paul Francis, Mark Handley, Richard Karp, and Scott Shenker, "A scalable content-addressable network," in *SIGCOMM '01: Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications*, New York, NY, USA, 2001, pp. 161–172, ACM.

[9] Julien Ridoux, Anne Fladenmuller, Yannis Viniotis, and Kavé Salamatian, "Trellis-based virtual regular addressing structures in self-organized networks," in *Proceedings of IFIP Networking*, 2005, pp. 511–522.