Position paper: Evolution Inspired Internet

Raimo Kantola, *Member, IEEE, Department of Communications and Networking, Aalto University*

***Abstract*—This paper looks at the Internet in the light of the theory of evolution. We note how the law of struggle for existence and natural selection has impacted the Internet. We pay more attention to the less well-known aspect of evolution, namely cooperation. We argue that the principles of cooperation that have served living organisms, particularly primates well in the past should and will be adopted more widely in the area of communications services over the Internet in the future in order to root out selfish behavior and business practices that are based on cheating. We show how this can be done and identify the challenges that lay ahead.**

***Index Terms*—Internet, wireless network, communications service, evolution, cooperation.**

I. Introduction

THIS paper takes a look at the present Internet in the light of the theory of evolution, characterizes the challenges the Internet is facing and proposes the principles for the Future Internet Architecture taking inspiration in the strategies for cooperation that humans apply. The paper discusses the solution from difference angles, draws some conclusions and identifies some directions for research.

Darwin's law of struggle for existence and natural selection is well known and has had a huge impact in philosophy, anthropology, social, political and many other areas of science. At first glance, the law favors selfish behavior since it is about survival of the fittest and ensuring continuation of one's own line of genes. Researchers in many areas of life science have been looking for a strong explanation why is it then that many living organisms from cells to primates and particularly people often behave altruistically and seem to cooperate more often than fight with each other. The cooperative behavior appears inside species and also between species. Cooperation is the opposite of selfishness and deceit.

In the 1980's Robert Axelrod popularized the results of game theory that showed how cooperation emerges as a winning and dominant strategy in a population with frequent interactions among the members. This was shown by repeated Prisoner's Dilemma games simulated on a computer. The same has been observed in numerous studies in biology, anthropology and the study of ecosystems (even in business ecosystems) (see e.g. [6]). It has been observed how the way to the dominant strategy of cooperation is not always straight. There may be oscillations between selfishness/deceit and cooperation. Particularly, when it is likely that a player will not encounter another player again, for maximizing the gains it may be best to be selfish and cheat. In evolution theory organisms do not engage in cooperation, because it is good. They do it because it turns out to be best for their survival. Morality and even forgiveness emerge as learned patterns of behavior in the long process of evolution when the conditions are suitable.

Among animals and organisms people are super cooperators. We have fine-tuned ways of recognizing our communication partner's oral and non-oral cues to make an assessment of the trustworthiness of the partner, we use language to express our opinions, we gossip about people to distribute our views and form a common opinion of people. Using this social intelligence we make selfishness and deceit loosing strategies in the struggle for existence. As a result, the "common good" – what is good for the species or the population as a whole prevails.

The rest of the paper is organized as follows: Section II looks at competition and cooperation in the Internet. Section III addresses the particular challenges the Internet is facing of the next 10 to 15 years. Section IV proposes the principles of the Future Internet Architecture. Section V presents some discussion of the solution. Finally, Section VI concludes.

II. Competition and Cooperation in the Internet

Let us take a look at the communications services over the Internet in the light of the theory of evolution. First we look at competition in technology and business planes and then observe how cooperative behavior of entities is either supported or missing.

In the current Internet, the network communications service is implemented with the combination of the Domain Name System and the IP protocol. Since TCP works between hosts, it is not considered as part of the network service. In a broader sense of the word, a communication service includes the host-to-host transport protocol as well as the communication application running on user devices and network servers.

A. Competition

From the history of the Internet we know about the survival of the fittest and natural selection. In this context we can observe technology battles and business competition. In the technology plane, only protocols that are widely adopted tend to evolve and survive in the long run while the niche protocols are forgotten. Also, the competition among applications is cut throat. Lately, we have seen how in certain services like

The author is with the Department of Communications and Networking in the Aalto University, Finland. (e-mail: fistname.lastname@aalto.fi).

search engines and social networking a dominant species have emerged and pushed the competitors into small niches. To summarize the technology battles: Internet has a strong tendency towards a dominant technology, service or protocol. Compared to typical natural ecosystems, the development is much faster.

In the business plane, the Internet forms a global ecosystem – users, service providers and network operators are all bound by the possibility of communication from any to any. This has been expressed in the form of the Metcalfe's law of network value. The trend over the past 15 years has been towards increasing role of global service providers such as Google and Facebook while the role of ISPs has been declining. The latest is the trend towards providing all or most services from the cloud. This development is driven by economies of scale in the Data Centers and the flat rate business model that has led to the mining of people's privacy, packetizing this information and selling it to advertisers. Such data mining can be best done in large data centers that serve millions to hundreds of millions of users. Taken further, this development is changing the Internet from an end-to-end network into an end-to-cloud network where the important relationship is from the user to the operator of the cloud. The economies of scale and mass market economies in processing power and memory can be best made use of in Data Centers rather than in network nodes – in this the raise of the cloud repeats the experience of earlier networks where the intelligence and value have been moving from the network to the terminals.

The network operators are tackling with the dilemma of how to maintain a measure of control over services provisioning and thus be able to make good on their investment into the network infrastructure. The model of services provisioning is moving from cooperation of network operators (like e.g. in mobile networks) to a dominance of a small number of global players each working in their segment. From the European perspective, it is worrying that none of the big global players at the moment are European. The key factor explaining this state of affairs is the lack of common digital market in Europe.

B. Cooperation

Let us then look at the other aspect of evolution, the phenomenon of cooperation in the Internet. The flip side is the lack of cooperation, i.e. the prevalence of selfish or even cheating behavior and what strategies are in place to prune out antisocial behavior.

The Internet uses collaborative methods to establish routes between the nodes. Also reliable communication using TCP is collaborative in nature, at least in theory. The collaborating partners are the hosts but they make assumptions of the network and in a way try to take the network into account. However, the hosts are guided by their interest to maximize their performance when using the network resources. The hosts are not supposed to maximize their performance selfishly over the interests of other hosts. In practice however, hosts can apply various methods in order to get more than their fair share of bandwidth from the network.

What comes to the underlying core protocol, namely IP, it ignores the idea of cooperation. Instead, it just offers the sender the possibility to send packets to anyone it pleases. The service is called Best Effort. Let us however be clear on this: the network makes its best effort solely in the interests of the sender.

So, the current communications service provided by the network is non-cooperative in nature. Unlike in face-to-face communication, there is no interaction with the receiver at the beginning in order to establish mutual willingness to communicate. The receiver can even not be sure who the sender is. The difference of the interests of the receiver and the sender can be expressed as:

Interest of Receiver = Interest of Sender – Unwanted traffic.

Compare the situation to voice networks: Mobile and ISDN networks have established an expectation that the callee can see the caller's number on his/her phone when receiving the call. At the beginning of a conversation it is customary to introduce yourself in order to establish a base level of expectations towards the other party. None of these routines apply to data communication over the Internet.

Users and corporate network administrators patch up IP's ignorance of interests of the receiver by deploying Firewalls in hosts and in network nodes. A Firewall uses local knowledge to filter incoming flows and packets. Modern firewalls are stateful. They routinely process flows using protocol specific state machines or application layer gateways (ALGs). These practices are seen unfavorably in the classical Internet "ideology". The argument against network-based firewalls is that they break the end-to-end principle and hinder the creation and deployment of new services. At the same time no amount of end-to-end talk will convince network administrators to get rid of their perimeter defense formed by Firewalls. In order to avoid this roadblock, most new applications are created to run over HTTP – a ubiquitous protocol that is allowed by most firewalls. This tends to ease the distribution of malware over HTTP and hinder the efforts of network administrators in protecting their networks.

The simplicity of IP opens an avenue for strategies that are based on deceit: hackers distribute Trojans e.g. using email attachments and special web sites, take control over other people's hosts, form botnets out of them and let other people use the botnets for the shady business of industrial espionage, spamming and fraud. More particularly, the dominant "services over HTTP" -development model is not particularly cooperative in nature. Rather it fosters competition but the downside is that it widens the avenue for the strategy of cheating using Trojans etc. The result of the weaknesses in the architecture is that a small fraction of Internet users are able to use cheating on a long-term basis to make money at the expense of other users.

The Internet has neither reliable and simple means of identifying the communicating entities, nor well-understood and recognized means of assessing the communication behavior of hosts, users or even ISPs, no means of gossiping

to form a common opinion of that behavior nor has it reliable and consistent social memory. Because of this, the Internet has no efficient strategy of making deceit and selfishness loosing strategies.

III. Challenges

According to ITU-T statistics, at the end of 2011 there were 2.4 Billion users on the Internet out of who half were connected using mobile broadband. This segment is growing fast and it is fair to expect that more than 90% of Internet connected devices will be wireless by 2020. Since the Internet architecture was created for fixed mains powered computers, (1) the challenge is how to adapt it to the emerging dominant mode of use. For example, the Internet Protocol itself does not support mobility. Instead add-on solutions must be used. The recommended mechanisms for NAT traversal lead to applications having to adopt networking specific code that wakes up the mobile periodically contributing to battery exhaustion. In addition the NAT traversal mechanisms are slow in connection establishment. Suitability to mobile use means that (1a) the architecture should have no components that force the mobile to wake up for non-user related reasons.

Another aspect of suitability to mobile mode of use that follows from (1a) is that (1b) no unwanted traffic should reach the mobile consuming its battery or disturbing the user. Due to this, the Firewall must be located in the network rather than on the device where it just depletes the battery even if it is doing its job.

The second (2) challenge is how to scale the Internet to a hundred devices per inhabitant of the world. The addresses allocation in IPv4 is now based on recycling since the free address space has all been allocated. IPv6 is proposed as the solution. However, IPv6 does not help to address the requirement (1b). IPv6 also requires that everybody should agree to use it. This has proven to be extremely hard to achieve.

Due to new services and more users, the Internet constantly needs more capacity. The challenge this creates is in (3) power consumption. Ethernet at 100 Gbit/s is now available and in about 2020-2022 we can expect 1Tbit/s Ethernet. Power consumption grows proportionally to the square of clock rate. The power consumption challenge can be best addressed by simpler forwarding modes in the core and pushing all complicated processing to the edge or to Data Centers where the consumed energy can be recycled to heat.

Finally, let us note the most important constraint on new technology for the Internet. It is (I) interoperability with existing application protocols and networks. Moreover, any new technology should be (II) incrementally deployable, i.e. one investor should be able to immediately benefit irrespective of what the other stakeholder's are doing.

IV. Proposed Solution

We propose (A) to extend the lifetime of IPv4 by Customer Edge Switching (CES) [1-3]. It is an extension and replacement of Network Address Translation. It is also a collaborative firewall managed by policy. A collaborative firewall is an extension of a stateful firewall that uses only local knowledge for admission decisions. In edge-to-edge communication CES introduces identities for the hosts, users and services. These can be of different types from anonymous IDs to Certificates. This makes it meaningful to collect data of the behavior of an entity and start forming a reputation.

The second component of the solution is (B) an Internet wide trust management system (see e.g. [4, 5]). Such a system collects gossip about the behavior of all entities: hosts, users, applications and ISPs and aggregates a collective opinion on the trustworthiness of each entity thus implementing a coherent social memory of behavior. The trust values of each entity can be used either for making administrative decisions or for making the entities pay for carelessness and cheating.

The solution addresses all the challenges as well as the two constraints listed above. It requires no changes in hosts.

A. Customer Edge Switching

Customer Edge Switching provides an interrupt driven access (challenge 1a). CES and an Internet wide trust management system like [4, 5] help to block unwanted traffic from reaching a mobile device. CES alleviates the IPv4 address exhaustion problem by allowing the use of any number of Private address realms to connect the new devices to the Internet (challenge 2). CES introduces a tunneling based edge. This makes technology choices in the core and in customer networks independent of each other making it possible to introduce new energy efficient forwarding technologies in the core (challenge 3).

A Customer Edge Switch can serve both clients and servers in the customer devices (like the User Agent Server in SIP) without the need to constantly keep alive a NAT mapping by polling. Instead, reachability is defined and managed by policy. CES is incrementally deployable (constraints A and B). We propose to start from Mobile Networks and Internet of Things whereby we can save a large block of IPv4 addresses and where the weaknesses of the current architecture cause most pain. It will be sufficient for those devices to have just private addresses.

We have implemented a demonstrator of the Customer Edge Switch on Linux and will make it available for the community at www.re2ee.org in the near future. The demonstrator offers the research user the scenarios of (a) a server behind a single CES and (b) clients behind one CES connected to another that serves the user's server hosts. The user will be able to test the interoperability with any protocol. The standard routines in CES are able to handle NAT friendly protocols (i.e. protocols that do not use IP addresses as IDs nor learn addresses or port numbers outside DNS) and we have implemented ALGs e.g. for FTP, SIP, ICMP. We have tested interoperability with SSH, HTTP(S) and Skype. Since we are targeting mobile devices and IoT at this stage, we argue that this is a sufficient initial set. We challenge the community to identify any protocols relevant to this customer segment that do not interoperate with our solution. Let us then design the

necessary ALGs together. These will be great student projects each.

CES introduces communications identities at the edge device. The protocol that tunnels customer packets from CES to CES supports many types of IDs from anonymous IDs to certificates. The protocol allows the inbound CES to make an informed decision on flow admission by asking additional questions of the outbound CES prior to admission. An example requirement of an inbound node is to require a certain or a certain type of ID. Using this capability it is easy to implement for example a service that we can call "me and my gadgets" – a VPN like security becomes available dynamically for a mobile user.

All communication and all control aspects of the traversal protocol edge to edge are policy managed. A lax policy does not impose any new restrictions, a tight policy requires verifiable identification of the sender, excludes CES routing locator spoofing etc. before admission. The policy rules can be chosen for each application separately.

Policies can be managed for example by the policy management architecture that has been developed for session-based services by 3GPP jointly with IETF.

B. Internet wide trust

In [4-5] we modeled an Internet wide trust management system that collects evidence of behavior from all hosts and also from network based monitoring systems. Internet Service providers aggregate the evidence and pass it onto a global trust service. This could be organized either based on a global agreement or within an alliance of operators. The trust service calculates trust values for all entities. One way of using the trust values is guiding network monitoring for collecting conclusive evidence and taking administrative actions against the detected bots. Another is using them to establish operator to operator and customer tariffs based on the trust value. The papers study different attacks on the trust management system and look for stability bounds under attack.

One of the tasks of the trust management system is to monitor the adherence of different networks to the semantics of the IDs that they issue. An example group of operators who could form a trust alliance is the GSM Association. In terms of distributing evidence or trust values the relationships of different alliances can be either: no exchange of information, asymmetric or symmetric.

V. DISCUSSION

In the short paper we do not attempt to give a proper review of prior art. We hope to do that elsewhere. Here we just compare our solution with Publish-Subscribe, which has been popular in the literature on Information Centric Networking. We argue that the general applicability of Pub-Sub is limited by the fact that the receivers (subscribers) either do not know what they want or cannot express their wishes in a concise manner as well as by the incentives of selfish publishers to cheat on what they are publishing. At the same time, the networking community has a long experience of policy-based systems. Customer Edge Switching can be seen to replace the subscription of Pub-Sub by a policy. Thus a CES based communication paradigm can be seen as a synthesis between the traditional Best Effort and Pub-Sub.

We anticipate the following main objections against the proposed solution: (1) Solution is firewall centric and creates new obstacles to innovation. (2) The solution requires ALGs and thus is not generic. (3) Identities require a new agreement between operators. (4) Why bother when most new intelligence will be in the cloud. (5) It is impossible to stop the forming of botnets. (6) The solution violates the end-to-end principle. We will address each of these objections one at a time.

(1) CES does not introduce the concept of firewall. It just makes existing firewalls smarter allowing them to collaborate before the final admission decision. In practice each operator hosting a CES service for its customers has to provide web access and admit HTTP(s). All applications over HTTP will be admitted as before. HTTP acts as the default admitted protocol. This will not change because of CES itself. But if a CES is integrated with DPI (or a stateful firewall is integrated with DPI), it is possible to block harmful applications running over HTTP. Use of such DPI depends on the administrators and the operators, not on the technology itself.

By supporting the establishment of some base level of assurances for a communication before admission, CES makes it easier for the administrator to make the admission policy decision than before. CES allows innovating on trusted services provisioning. The arguments show that CES opens new avenues for innovation rather than hampers innovation.

(2) CES architecture proposes that an application designer has a choice: (a) design a new protocol that is NAT friendly to run over e.g. HTTP and thus bypass firewalls or (b) besides the new protocol, design and publish also the necessary ALGs and policies for the CES-like firewalls. It will then be up-to the operators an network administrators to verify the ALGs and policy templates and provision the services to users who subscribe to the new service. The operators can use their policy management architecture to let the ALGs and the policies follow the users as they roam in foreign networks. How to implement this best in CES software is a development challenge. By offering firewalling services from a cloud, operators can ease the burden on corporate network administrators. Option (b) may make sense when the nature of the service or application is such that it requires a high level of trust between the communicating parties.

(3) Since CES supports many types of IDs, some of them can be provided by corporate network administrators on their own or by mobile operators leveraging their existing infrastructure. It is true that for enforcing a strict semantics of an ID type, an agreement between the players is needed. Such agreements can be formulated once the technology has been tested; the protocols have been standardized and are supported by many vendors. An Internet wide trust management system helps to monitor the adherence of the players to the semantics of the IDs and punish for misbehavior. Thus minimal deployment of CES technology requires no new agreements

between operators. However, for making the best use of the technology such agreements are indeed useful.

(4) Communication still requires that there is a source and a destination. A mobile device will host several communications applications that can attach to several networks. How to be reachable in each of those networks using any of the communications applications still needs to be addressed. Cloud based services intelligence does not change this in any way. Moreover, cloud based services work in places with a certain level of trust. It is not clear that they will be adopted everywhere.

Internet wide trust management is a suitable application for implementation in the cloud. It would leverage the power of centralized cloud based architecture for improving the cooperation of customer networks for a common good – i.e. curbing the impact of selfish behavior and cheating on the Internet.

(5) CES together with an Internet wide trust management system can help to locate each bot quickly reducing the "useful" lifetime of each bot. The more active a bot is, the faster it will be spotted. This will limit the scope of strategies that are based on cheating. The fact is that there are wide variations in the share of bots in different OECD countries: OECD average bot penetration in 2011 was 1.5% while in some counties more than 5% of hosts were infected. This tells that if ISPs and users become incentivized to be more careful, the distribution of Trojans becomes much more difficult than now.

(6) If Customer Edge Switching is adopted in all networks that connect customers to the Internet core, the resulting network is still called the Internet and it will still be based on the end-to-end principle. We should refine our understanding of the Best Effort service. The idea is that the network should make its best effort for both the sender and the receiver instead of just the sender. There is no good reason why a function that cannot be effectively implemented in a (mobile) host, should not be implemented in the network.

VI. Conclusion and Research Challenges

We gave a quick review of the current state and the technology of the Internet in the light of the theory of evolution. We suggest that the global Internet ecosystem behaves similarly to other ecosystems. As more advanced species are more likely to adopt a dominant strategy of cooperation in place of systematic or occasional cheating, we suggest that on the evolution path of the Internet, it is time to look for smarter methods of cooperation between the entities that participate in communication. The smarter methods of cooperation should target curbing the selfish and cheating strategies used by hackers, spammers and fraudsters. To this end we propose two new components: (A) Customer Edge Switching that acts as a cooperative firewall and (B) an Internet wide trust management system. The first makes the basic act of communication receiver-friendly, establishes identities for the hosts and allows eliminating address spoofing. The latter allows identifying customer networks. Once the identification of the entities is easy, it makes sense to collect information on the behavior on the entities and start forming a coherent opinion on the reputation of the entities. This is the task of (B).

CES mimics the kinds of methods people use to establish a level of trust at the beginning and during a conversation or any social interaction. This draws on the human history how we have managed to move from war of all against all to a dominant cooperative behavior (see e.g. [7]).

An Internet wide trust management system mimics our collective opinion or social memory of other people's behavior. This draws on the human competences of using language to describe a behavior, gossip about it and prune behavior that is seen as anti-social by the majority. These are the kinds of traits that have made humans super collaborators. We claim that it is possible to draw on this social experience and to an extent mimic it in network-based software.

A. Research Challenges

The soon to come demonstrator will show that the core functionality of Customer Edge switching indeed works. The research challenges related to our proposed solution are still numerous. I will name a few.

(a) The concept of Customer Edge Switching needs to be applied to different network contexts. For example nested or hierarchical CES may be useful in some of them. The procedures for robustness and multi-homing need refinement. (b) Full integration of CES with the existing policy management methods using Diameter needs to be developed. (c) Formal modeling of collaborative firewalls and their policies will be useful and will help in designing effective policies. A more technical topic is how to best leverage the existing policy management architecture of mobile operators for managing the collaborative firewalls.

Finally, on the Internet wide trust management we have done only initial work. It needs (d) full integration with all kinds of tools that have information that is useful "gossip". (e) Definition of the language for gossip. Also (f) different architectures of the trust management system should be studied.

References

[1] R. Kantola, www.re2ee.org.

[2] R. Kantola, Implementing Trust-to-trust with Customer Edge Switching, AINA 2010, WS on Advances in Mobile Computing and Applications: Security, Privacy and Trust, Perth, Australia.

[3] M.Luoma, R.Kantola, J. Manner, Future Internet is by Ethernet, Networks of Future, World Computer Congress, IFIP, Brisbane 2010.

[4] Z. Yan, R. Kantola, Y. Shen, Unwanted Traffic Control via Global Trust Management, IEEE TrustCom2011, Changsha, China.

[5] *Z. Yan, R. Kantola, Y. Shen*, "Unwanted Traffic Control via Hybrid Trust Management", IEEE TrustCom 2012, Liverpool, UK, June. 2012.

[6] Martin A. Nowak, Why we help, American Scientist, 7/2012.

[7] F. Fukuyama, the Origins of Political Order: From Prehuman Times to the French Revolution, Farrar, Straus and Giroux, 2011.