Cooperation and End-to-End in the Internet

Raimo Kantola[1], Hammad Kabir[1], and Patrick Loiseau[2]
[1]Department of Communication and Networking, Aalto University
[2]Network and Security department, EURECOM

Abstract: This paper analyses the motivation and strategies for ensuring cooperative behaviour among hosts and customer networks in the Internet and 5G networks. The hypothesis is that better cooperation among the benevolent entities could improve the overall Internet welfare, motivating the need for adoption of cooperative security. However, in state-of-the-art, the prevalent security approach in the Internet is based on self-help, while the adoption of cooperative methods is progressing slowly. At the same time, the ubiquitous reliance on 5G and mission critical nature of some of the new services, for example, ultra-reliable (machine-to-machine) communication and Internet of Things, requires that 5G will do its best to curb the malicious (non-cooperative) behaviour from becoming a cause of failure to the legitimate services. In this paper, we relate our analysis of the conditions for sustainable cooperation in the Internet with the famous end-to-end principle, and present the hypothesis that *there is no end-to-end solution to the problem of ensuring cooperation among Internet hosts*. Game theory allows studying the outcomes of interactions among the players with conflicting interests. We use it to study the hypothesis, and show that introducing the reputation of Internet nodes and customer networks can lead to cooperation, which improves the overall Internet welfare and reduces the payoffs of malicious actors. We study the possible response of *non-cooperative* users with advanced defection strategies and the resulting outcomes. We argue that 5G shall make significant progress towards uprooting the selfish behaviour and malicious activities using cooperation and relate it with motivation for providing ubiquitous connectivity and ultra-reliable services. The paper concludes by summarizing our earlier work on the application of the proposed methods of cooperation to 5G and the Internet; outlining how cooperation in security is not only desirable but also feasible.

Keywords: 5G, Internet, ISP, cooperation, game theory, security, communications service, networks, evolution.

1. Introduction

The ITU-T statistics [1] indicate 3.5 Billion individual Internet users; the number of active mobile broadband subscriptions has recently overtaken this number. This segment is rapidly growing, and expectedly the number of Internet connected wireless devices will increase. The initial estimates for 5G are to handle nearly 100 devices per inhabitant of the world and that the data traffic will grow 1000-folds from 2010 to 2020 [2-3]. Similar to LTE, the traffic in 5G will be packet switched. These considerations lead us to a key premise: 5G will be a new phase in the evolution of the Internet. This implies that in designing 5G we should relate the design to the Internet principles.

The most famous Internet principle is called the *end-to-end principle* [4]. It states that if a function cannot be completely implemented in the network, it should be left to the end hosts. This principle has a central role in keeping the network simple, and it has facilitated user innovation by allowing the users to create some smart software to address their needs; instead of relying on the operators to recognize, understand and address the needs. This has been very successful because users largely operate on very competitive consumer markets, while the operators procure their equipment and software on investment goods markets with

slow cycles and high prices.

End system software is often poorly developed and contains un-patched vulnerabilities that put the hosts and their corresponding networks at risk. Since there is no certification for the software running on end-hosts, best practices are often ignored in the software development, and security is mounted at the end rather than being part of the development cycle [5, 6]. Furthermore, Internet connected devices may lack functions for easy upgrade of their software. Consequently, Internet is suffering from hacking attempts into the end systems, to connected cloud-based systems, fraud, theft of user information and corporate IPR, spamming, denial of service attacks [7] etc. We label all these forms of behaviors and hosts/agents used by the hackers, as *non-cooperative*. Most of these practices are outright illegal, but enforcing law on the Internet has proven to be challenging: the probability of identifying an attacker is low. Smart mobile devices, and in particular 5G, further aggravate the situation, such that the end systems become even more lucrative for attackers. New ways to benefit from the non-cooperative and illegal activities will emerge, as the users will routinely store confidential information and execute monetary transactions from these devices and corporations will build the Industrial Internet.

In comparison, the prevalent attitude in security is based on self-help, such that the owner of the host or the customer network concerns with its own security and does not cooperate with others or cooperates no more than the required regulatory compliance. Some efforts by system security vendors and regulators have resulted in limited cooperation in security, for example: for sharing of vulnerability information and establishing CERT [8] for security incident reporting. However, the adoption of cooperative methods is progressing slowly.

This paper addresses the research problem of understanding the impact of cooperative security on the welfare and strategies of both benevolent and malicious Internet users. The paper evaluates whether the efforts towards better cooperation among benevolent entities could contribute to the overall Internet welfare. The purpose is to use the development of welfare of Internet users as basis for adapting a more cooperative approach to Internet security, compared to the current practice.

This paper argues that it is not enough that we secure 5G networks. Instead, we argue that the networks should do their best to curb the non-cooperative behavior of a small portion of the Internet users and hosts. We study the question: whether we can achieve this and address the problem by applying the end-to-end principle. By reviewing the literature on the theory of cooperation, we build a hypothesis that there is no end-to-end solution to the problem of ensuring cooperation among Internet hosts.

To support our hypothesis, we study the outcomes of interactions between benevolent and malicious Internet hosts by applying Game Theory [9], which provide necessary tools for studying interaction of the players that attempt to maximize their welfare and often have conflicting interests, similar to the hackers and nice users in the Internet. We present the game-theoretic analysis of the cooperative and advanced non-cooperative strategies that Internet entities can adopt; and study their impact on the Internet welfare. The analysis motivates to create and deploy a system of indirect reciprocity based on a generic reputation system for cooperation between Internet entities. We study the contributions of such a reputation system with repeated Prisoner's Dilemma simulations. The paper shows that it is possible to make Internet hosts cooperative in nature and this can lead to a sustainable increase in the Internet welfare. This is possible due to global sharing of the misbehavior evidences via reputation system, which limits the scope of defection strategies in the Internet and thus leads to lower defection gains. Our earlier work [10-12] studied the

question of robustness of such an Internet-wide reputation system under system attacks. In [13-14], we studied the deployment aspects and focused on the business dynamics of the actors that may need to invest into Internet-wide trust. This paper complements our earlier work by analyzing the overall impact of the reputation system onto the value of the Internet. If we conclude that the value increases, as shown in Figure 1, this bodes well for adoption.

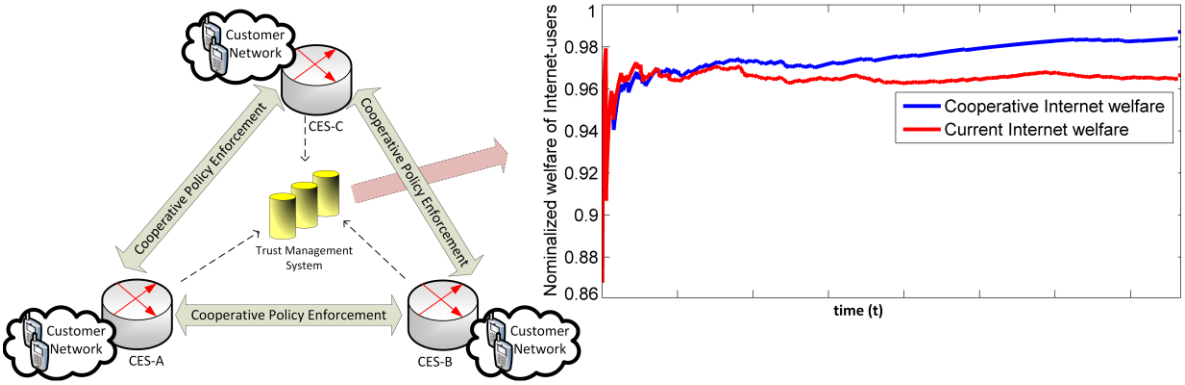

Figure 1. Internet-wide reputation system could lead to sustainable increase in the Internet welfare

The timeliness of this research relates to 5G, which will expectedly support new models for provisioning network and communication services. The major drivers of security in 5G come from: a) new trust models; b) new service delivery methods; and c) evolved threat landscape. While the support for new use cases will change the current trust models and raise serious security considerations for 5G, the evolved threat landscape would challenge the thriving potential of new services that would rely on 5G for ubiquitous connectivity. Mobile networks already today rate availability as their top concern [15]. The evolved threat landscape of 5G will further stress this concern, since new use cases could be supported by new market entrants with varying level of security understanding. For example, the early work on 5G [3] sets the requirement on supporting massive machine-to-machine communications and ultra-high reliability, for example in life-critical automotive applications. There is a concern that these applications will put human life at stake and make it possible to sabotage major industrial value by hacking into the connected machines. Thus, 5G faces huge load of managing the expectations, i.e. connectivity, and yet ensuring security and cooperative behavior of its hosts [16]. We argue that the goal for 5G is not to have a faster mobile broadband network, where legitimate services may fail due to malicious activity that uses almost trivial attacks. It is pertinent that 5G makes significant progress in protecting the legitimate hosts and services from attacks, compared to the state-of-the-art.

To outline the feasibility of cooperation among Internet networks, the paper briefly describes the implementation of our solution particularly in 5G. The overall two-tier security solution proposes: 1) a network-based firewall (Customer Edge Switching [17-24]) that addresses inherent Internet vulnerabilities and security at the level of interaction between customer networks; and 2) an Internet-wide evidence collection, aggregation and reputation system. This paper concerns with the latter, i.e. *Internet-wide reputation system*, which aggregates the evidence of misbehavior from trusted network entities (such as Customer Edge Switch), and besides source reputation generates indicators for trusted network monitoring to lower the Internet defection gains. Comparing the simulated welfare of Internet under cooperation with the current Internet, we predict reduced threat levels and improved welfare for Internet under cooperation, and argue that 5G shall make significant progress in this direction. Such need for cooperation in 5G also emerges from new use

cases, where multiple players or service providers would need to cooperate to deliver their services. The paper also studies the possible responses of non-cooperative users and the ways in which cooperative entities can maximize their welfare, besides discussing the deployment aspects of our approach.

The rest of the paper is organized as follows. Section 2 summarizes the major results of the theory of cooperation in different studies and presents how they can be applied to foster conditions for sustainable cooperation in the Internet. We build on this to formulate the key hypothesis for this paper. Section 3 overviews the theoretical frameworks and models used in the Internet security research, and discusses suitability of the game theory for studying our research problem. Section 4 models the interactions between hackers and normal users, and elaborates how welfare develops in Internet as a function of the hacking interactions. The section also formulates the detailed research questions for this paper. Section 5 presents a game of hackers and nice users in the Internet, suggesting a sustainable increase in the Internet welfare under cooperation. Section 6 describes our solution and approach for promoting cooperation among the Internet entities, and Section 7 concludes.

2. Background – studies on cooperation

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 fields 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 seeking a strong explanation of 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 opposing each other. The cooperative behavior appears inside species, at cell level, and also between species. It can be studied in groups of players or in the whole ecosystem. Cooperation is the opposite of selfishness and deceit. In the following, we recap major results of the theory of cooperation and highlight key findings in the form of 4 rules.

A classical game for studying the conditions that lead to cooperation is called the Prisoner's Dilemma [25-26]. The underlying assumption is that each player will pursue maximizing its payoff. Table 1 defines the payoff matrix for two players:

Table 1: Prisoner's Dilemma

	Cooperative	Non-cooperative
Cooperative	(c, c)	(s, t)
Non-cooperative	(t, s)	(e, e)

where the inequality t>c>e>s applies.

In this game, the biggest payoff (t), called temptation, is earned if one manages to defect when the other player chooses to cooperate. The next largest payoff comes from mutual cooperation (c) followed by the case of mutual defection (e). The worst payoff (s) is called the sucker's payoff, obtained by a cooperative player upon interaction with a defecting entity. The solution of the single round of this game is mutual defection, which is socially un-optimal.

In the 1980's, using computer simulations of a multi-round Prisoner's Dilemma, Robert Axelrod [26] popularized a major result of game theory showing how

Rule 1: cooperation emerges as a winning and dominant strategy in a population with un-ending sequence of interactions among the members.

This result confirms the empirical observations with the outcome of computer simulations, based on a mathematical description of the interactions. Outcome of an un-ending multi-round game is opposed to a single-round game, where the equilibrium is mutual defection. The multi-round game assumes that *those who win the most benefits will multiply and/or that the participants learn to apply winning (cooperative) strategies from previous rounds of the game*. A similar emergence of cooperation has been observed in numerous studies in biology, anthropology and the study of ecosystems (even in business ecosystems) (see e.g. [27]). Social studies and experiments show that people have a strong inclination to choose to cooperate – however, this does not apply to all individuals without exception [25, 28]. It has been observed that the path to the dominant strategy of cooperation is not always straight. Particularly, when

> *Rule 2: it is likely that a player will not encounter another player again, for maximizing the gains it may be best to be selfish and defect.*

This corresponds to the solution of a single-round Prisoner's Dilemma game and thus the result is not surprising. Moreover,

> *Rule 3: if enough players simply refuse to cooperate, cooperation in the group may fail completely, i.e. a socially un-optimal strategy becomes dominant. We call this cooperation failure.*

To avoid this cooperation failure [29],

> *Rule 4: often members of the group or society must be ready to sacrifice the immediate benefits, in order to punish the violators of cooperation.*

For example, we can take the last two rules to explain why organized societies need law enforcement and prisons, although they cost a lot. Irrespective of the cost, in the long term, the society as a whole will benefit [30].

In the evolution theory, organisms do not engage in cooperation, because it is "good" or moral, rather because it turns out the best for their survival. Among animals and organisms, people are super cooperators. We have fine-tuned ways of recognizing our communication partner's oral and non-oral cues for assessing 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. These methods help us avoid being cheated. Moreover, using 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, a group or society as a whole, prevails. Social structures such as large companies, states, religions and international organization such as EU, UN etc. are a testimony on how successful people are in cooperation compared to other primates on Earth. Societies that exhibit a high level of internal trust among people have low interaction costs and are capable of forming highly successful organizations with flat structures and high level of horizontal interactions. Such organizations are efficient, for example in knowledge-centric work. At the same time, we observe failed states and wars as examples of cooperation failure.

Considering whether the conditions for cooperation becoming the dominant strategy required by *Rule 1* are directly in place among the users of the Internet, we observe that they are not. Due to the flat any-to-any addressing of IP, any unknown user can send traffic to any stranger. The sender typically uses a dynamically assigned address or even worse, it is often able to spoof its address and *hide*. Under these premises, the interaction is not un-ending. Consequently, game theory tells us that largest benefits are gained by defection

(*Rule 2*). Thus, we claim that

Claim: there is no end-to-end solution to the problem of ensuring sustainable and long-term cooperation between users of the Internet.

The arguments for this claim are that (a) pre-requisites stated in *Rule 1* are not directly in place among the Internet hosts. Logically, it does not follow from *Rule 1* that cooperation could not emerge under some other conditions not presented in *Rule 1*. In fact, the most famous principle applied to Internet is the end-to-end principle: it states that if a function cannot be completely implemented in the network, leave it (entirely) to the end systems.

However, (b) *Rule 2* and the outcome of a single round of Prisoner's Dilemma shows that if interactions are not un-ending, it is often best to defect. Conditions for *Rule 2* are in place in the Internet, because of the lack of the long-term memory, poor sharing of the outcome of different strategies and weak identification of hosts. The wide penetration of Trojans, tussle for more than the fair share of bandwidth are examples that confirm the theoretical results (*Rules 1* and *2*) and our claim. In subsequent sections, we will model the state of the Internet and add an Internet-wide reputation on top to examine its impact on the end-user welfare. We see the reputation as a way of introducing classical methods that people and other primates use to improve cooperation in a group or the society. By analyzing the Internet welfare and its development under cooperation, we motivate deploying the methods of cooperation in the Internet and 5G.

We argue that the resulting Internet would be more suitable to act as the critical infrastructure of a modern society: people, companies and connected machines would be able to rely on the network to do more in much varied contexts than today. We argue that 5G should aim to make significant progress in this direction: the goal should be minimizing the risk of failure of a legitimate service due to malicious activity. We argue that this is in accordance with the requirements of 5G for supporting ultra-reliable communications.

3. Related Work

The emergence of cooperation among primates has attracted interest from scientists and researchers in various fields, such as biology, anthropology and social studies. Often, this has been studied under the framework of evolutionary game theory [31]. While the other closely related frameworks such as Decision theory [32] and Rational Choice [33] have studied the (impact of) choices and strategies by individuals in an attempt to maximise their welfare. The evolutionary game theory is concerned with the interactions of its players and assumes that survival of a strategy in a population depends on the benefits achieved by its adherents. In addition, it provides a set of tools to model interactions [34] between self-interested agents that aim to maximise their gains and often have conflicting interests.

Game theory has been used to study the challenges in communication networks [35], where the interaction is amongst self-interested hosts. The analytical tools provided by game theory have addressed a breadth of areas, such as distributed resource management, congestion control [36], the network layer issues [37] and spectrum sharing [38] in the cognitive networks between secondary users. Similarly, the models and analytical tools provided by game theory have found their application in Network Security [39]. For example, the authors in [40-41] apply game theory to network intrusion detection systems.

The suitability of game theory to study Internet security challenges comes from the fact that a player's outcome in the game theory depends not only on its actions, but also on the actions of its opponent. This is analogous to the Internet, where the strength of a host's security is a function of its own security strategy as well as attacker's proficiency. A typical

security analysis using decision theory assumes that the defender views the attacker's actions as exogenous [42]. For example, the strategy of attack or its probability is provided as an input to decision-theoretic model. For this reason, decision theory is often described as a *game against nature*, where nature is an opponent that does not seek the best payoff, rather acts independently [43]. In comparison, both the security choice and attack strategy are endogenously determined in a game-theoretic model, making it suitable for modelling interactions with dynamic and pro-active adversaries, such as hackers [44]. Another closely related discipline, Rational Choice theory assumes that the players act *rationally* (i.e. as per their strategy preferences) while they attempt to maximise their utility. However, it does not provide the necessary tools to address the issue at hand: to model Internet interactions and study the development of welfare as a function of hacking interactions [45].

The game-theoretic research to study the communication security problems is generally classified in two groups. The first group leverages the basics of game theory to study the foundations of the security problem and derive technical solutions. The other set considers socio-economic aspects of the security and studies the incentives, behaviour and economics of the agents i.e. host or attackers, involved in the Internet security [44]. In this paper, we leverage game theory to describe the research problem and present a solution that contributes to Internet welfare, by affecting current incentives of the Internet players.

The research in [39, 45] presents a taxonomy of game-theoretic models. It classifies game theory research to: cooperative/non-cooperative, sequential/simultaneous, finite/infinite and evolutionary nature of the interaction between players of the game. Game-theoretic research to network security typically employs non-cooperative models, where individual players are the units of analysis. This is in contrast to the cooperative or coalitional games that analyse a group of players against defecting entities. Since single-shot game theory suggests socially un-optimal *defection* as the best strategy, researchers often employ infinitely repeated game-theoretic models to study the evolution of cooperation [26]. We leverage a *multi-stage infinitely repeated non-cooperative* game-theoretic model in this paper, to study the evolution of cooperation in the Internet. Here, game theory allows modelling of Internet interactions between players (hackers and nice users), while multi-stage infinitely repeated nature of the model allows studying the evolution of cooperation at the level of individual interactions.

Traditionally computer tournaments have been used to study the evolution of cooperation. In such tournament experiments, many strategies compete. Often the winning strategy that emerges dominant is *tit-for-tat* [26]. A player following this strategy will first choose to cooperate and will never defect/cheat first. If the player is cheated upon, he will remember this and respond in kind in the next interaction: players have a memory of the previous round with the opponent. The experiments show that, for example, the strategy of 'turning the other cheek' will perform worse than tit-for-tat leading to low overall welfare. Lately, a high performing strategy called *Win-Stay, Lose-Switch* (WSLS) was proposed [46]. This strategy is more aggressive than tit-for-tat and allows repeated defection, if the other party does not retaliate. The paper in [45] discusses different strategies for evolving cooperation in a group: 1) Direct reciprocity uses the *tit-for-tat* strategy; 2) indirect reciprocity refers to deploying a system so that a defection attempt against one player is perceived as a defection against whole population; and 3) under spatial reciprocity co-operators form clusters to resist defection attempts from defectors.

Unlike the traditional evolutionary game theory that allows learning new strategies and possibly converging on a dominant strategy, we aim to study the welfare of Internet entities. Such welfare or utility analysis is often employed in research [48-51], and we will use it to address some key research questions of this paper, besides revealing the development of

welfare in the Internet. The welfare analysis will motivate towards an Internet that can more suitably act as a baseline for studying choices presented by Decision Theory and Rational Choice, i.e. end-users can adopt strategies to improve their security, e.g. in accordance with the *rational* values of their society or population. The paper complements the work in [25] by conducting quantitative analysis of the problem of cooperation and presenting a pathway towards achieving sustainable cooperation in the Internet.

Our approach for attaining sustainable Internet cooperation offers a different perspective from proposals like Accountable Internet Protocol (AIP) [52]. AIP attributes the malicious activities and Internet attacks to the lack of accountability in the Internet, and proposes to replace the Internet protocol (IP) so that user actions can be accounted and attributed to a certain Internet entity. The solution relies on the adoption of self-certifying addresses for Internet domains and end-hosts, which can be a major deployment challenge. Besides the compatibility challenge with routing infrastructure, AIP further worsens the problem due to its reliance on flat addresses that makes CIDR-like address aggregation impossible. In comparison, our proposed approach limits all the changes to the edge network nodes and addresses classical weaknesses of the Internet, namely source address spoofing and denial of service attacks, without requiring any changes to the end-hosts. This paper describes how we can achieve this based on a certain role of network-based firewalls and an Internet-wide reputation of the communicating entities.

4. Modelling the Internet Interactions

This section leverages game theory fundamentals to model the interactions between hackers and ordinary Internet users. We lump all the malicious actors as *hackers* that use the Internet for breaking into computer systems, stealing information, fraud, service denial and for spamming. Hackers mostly employ bots – i.e. malicious software running on other Internet hosts to launch their attacks. We define a two-player game to model the Internet interactions, where each player can either assume the role of a nice user or a hacker. By normalizing the payoffs to the average benefit of communication between two nice users, we define games A and B in Table 2.

Table 2. Payoff matrices for the game of nice users and hackers

A	Nice guy	Hacker
Nice user	(1, 1)	(s, t)
Hacker	(t, s)	(0, 0)

B	Nice guy	Hacker
Nice user	(1, 1)	(s, t)
Hacker	(t, s)	(r, - r)

where the row player's payoff is the first and the column player's payoff is the second in each element of the payoff-matrix. In the game, t is the temptation payoff and s the sucker's payoff. We note that we can only model active bots while the dormant bots that just wait for an activation command cannot be accounted by this model.

In the game, we argue that a hacker does not create value from nothing. Rather, hacking can be compared to stealing, where some value changes hands. In the process, some of the original value is lost. Therefore, $t < |s|$ holds, where s is negative. In game A, we average out the payoff for the case when two hackers meet over the host of a nice user. This is because in infinitely repeated games that span over multiple rounds, the sum of payoffs in this element of the matrix approaches zero. However, game B depicts the case of two hackers interacting in a single-round game, where the row player wins control over nice user's host from the column hacker. The winner gains the residual value of the bot (r) and the looser looses the same amount. It is reasonable to assume that $t > r$ because the host has already been compromised and nice user disturbed, so the likely remaining lifetime of the

bot in the machine of the nice guy is less than the case of taking over a fresh and un-infected machine. Besides, the value of the information that is stolen the second time is less than the case of fresh infection.

For game A, we observe that $t > 1 > 0 > s$, i.e. the game is Prisoner's Dilemma [25]. This observation does not depend on the relation of absolute values of t and s. The variant B of the game allows looking at relations of different hackers, in addition to the interactions between nice users and hackers.

Based on this, we conclude that the classical results of game theory can be applied to the state of the Internet when it comes to modeling the relations of hackers and rest of the users, with some considerations. Expectedly, both the strategies: cooperation and non-cooperation will be sticky in the Internet: ordinary users usually choose to cooperate and will not act illegally; and the hackers have chosen to make a living out of hacking and are not easily deterred because being caught is unlikely. Another major difference for Internet, compared to the tournaments in [26] for studying the evolution of cooperation is that sharing of the results of the games is weakly developed in the Internet. Recording the outcomes against a player would require a stable identity that is normally not available in the Internet. Therefore, learning based on the earlier outcomes is slow (or works poorly) in Internet.

Contrary to the evolutionary game theory that concerns with learning new strategies and players possibly converging on a dominant strategy, we aim to present the welfare analysis of the Internet players: hackers and nice users. This is because: (a) stickiness to the strategy choices by players causes unwillingness to learn new strategies; (b) even if willing, learning is difficult due to weak identification; and (c) lastly, it would seem unethical to possibly suggest nice hosts to become hackers or advice the hackers to improve their strategies. Based on this initial analysis, we pursue with welfare analysis of Internet players and identify the following research questions for this paper.

(1) How does the overall welfare develop as a function of the share of successful hacking interactions?
(2) Is there an optimal level of successful hacking that yields the best overall outcome to (the brotherhood of) hackers?
(3) How does the split of welfare between the hackers and the ordinary users develop as a function of the share of successful hacking interactions?
(4) What is the outcome if we introduce better ways of sharing the results of the game, i.e. a reputation system that spans to all Internet hosts and is trustworthy? Does this change the way welfare is distributed between the both types of players?

We address the first three research questions with game-theoretic welfare analysis. Section 5 addresses the last question using a simulation of a multi-round game.

4.1 Analysis of overall welfare

For the welfare analysis we can use game A, because for a large number of hacker-to-hacker interactions over host of a nice user, the sum of payoffs in that element of the matrix is clearly zero.

Let I = set of all the interactions over the Internet during a rather long period of time. We assume the interactions are always between two hosts/users. Multi-user interactions can be split into the constituent paired interactions.

In a random interaction in *I*, the value offered by a cooperating activity is $v_c = 1 - h + hs$,

where *h* is the share of successful hacking interactions in *I*. We ignore the cost caused to hackers by their bots upon sometimes failing to infect a nice guy or receiving a defection gain in the interaction. These costs are factored into the hacker's gain *t*. The payoff from hacking activity in a single random interaction in *I* is

$v_h = ht$,

The total value from a random interaction in *I* is:

$$v = 1 - h + hs + ht, \quad (1)$$

The total value over the whole set of interactions is then:

$$V = v \times |I| \quad (2)$$

It is reasonable to assume that the ordinary users will cease to use the Internet long before all interactions lead to successful hacking. We will assume that all ordinary users will cease to use the Internet when *h* reaches h_{max}, where $0 < h_{max} << 1$. By deduction we figure that $h_{max} < 0.1$. At this point, each 10th interaction would lead the ordinary user loosing control of the information on his machine, as well as the control of the machine itself.

We approximate $|I|$ as:

$$|I| = I_0(1 - (\beta h)^2), \quad (3)$$

where I_0 is the size of the set of Interactions in a relatively long unit of time (e.g. a month) when there is no hacking. When the share of interactions (*h*) leading to successful hacking of an ordinary user's host starts to grow from zero, initially the hacking activity has little impact, but after a certain threshold, hacking starts to have a negative effect on the adoption of the service until the usage drops dramatically and ceases altogether when *h* reaches its maximum:

$$h_{max} = 1/\beta. \quad (4)$$

This model is simplistic and does not try to model the process of the service collapse accurately. It may also be more appropriate to make the process of collapse more abrupt than what a quadratic polynomial can model. Nevertheless, let us use the approximation to make some qualitative analysis.

Moreover, we can model the hacker payoff $t = B + g\tau$ where τ stands for the lifetime of a bot. This can be interpreted such that the payoff of the hacker consists of the value of the stolen information, extortion, or fraud (B) that can be done with the information and of a time dependent component reflecting activities, such as network scanning, bot distribution, spamming and use of bots for DDoS and other purposes through the bot-rental business. This latter component is in direct proportion to the lifetime of a bot.

The value of all interactions in a time unit is therefore modelled as:

$$V = (1 - h + hs + ht) \times (1 - \beta^2 h^2)\, I_0. \quad (5)$$

We normalize this by dividing both sides by I_0, denoting the normalized value by *w*.

$$w = (1 - h + hs + ht) \times (1 - \beta^2 h^2). \quad (6)$$

Let us further denote: $d = 1 - s - t$. This is the difference that a nice user has at stake and what a hacker can obtain in an interaction over the Internet. Because the value of a single interaction over the Internet to a nice user is positive and $|s|>t$ on average, we can reasonably expect that $d > 0$. Then,

$$w = (1 - dh)(1 - \beta^2 h^2). \quad (7)$$

For analysis, we split the function into three areas to study how harmful or profitable hacking is. Useful ranges are: (a) hacking destroys a lot of value, $d \geq \beta$; (b) normal case, $0 \leq d < \beta$; (c) hacking is more profitable than we expect, $d < 0$.

Case (a): The normalized welfare declines to zero at $h = {}^{1}/_{d}$. Because hacking destroys a lot of value, collapse of the service takes place earlier than predicted by β alone. De-facto, this means that the model of decline set by the factor $(1 - \beta^2 h^2)$ is not accurate in this case.

Case (b): For analysis, we derive the first and second derivatives of the function *w*. By default, this provides the minimum/maximum values for *w*. The derivatives are:

$$\frac{dw}{dh} = 3\beta^2 dh^2 - 2\beta^2 h - d. \quad (8)$$

$$\frac{\boldsymbol{d^2 w}}{\boldsymbol{dh^2}} = 6\beta^2 dh - 2\beta^2 = 2\beta^2(3dh - 1). \quad (9)$$

Roots of the first derivative are $h_{1,2} = \frac{2\beta^2 \pm \sqrt[2]{4\beta^4 + 4 \cdot 3\beta^2 d^2}}{6\beta^2 d} = \frac{\beta \pm \sqrt[2]{\beta^2 + 3d^2}}{3\beta d}$. (10)

The first root is positive and the second is negative, so the latter falls out of the range for *h*. Let us show that the first root is out of range $h \in [0, h_{max}]$. In this case, following shall hold:

$$h_1 > {}^{1}/_{\beta} \Rightarrow \frac{\beta + \sqrt[2]{\beta^2 + 3d^2}}{3\beta d} > \frac{1}{\beta}$$

Because both β and *d* are positive, we can multiply the inequality by the denominator of the root.

$$\beta + \sqrt[2]{\beta^2 + 3d^2} > 3d \implies \sqrt[2]{\beta^2 + 3d^2} > 3d - \beta.$$

When $0 \leq d < \beta/3$, the inequality is always true. In the range $\beta/3 \leq d < \beta$, the inequality can be expanded to:

$\beta^2 + 3d^2 > 9d^2 - 6\beta d + \beta^2 \Leftrightarrow \beta > d$, which is true. Hence, h_1 is out of $[0, h_{max}]$.

Since there is no local minima in the range $[0, h_{max}]$, we interpret that in case (b), the value *w* declines monotonically. For this case, if we denote $\beta = \alpha d$, the factor $\alpha = {}^{\beta}/_{d}$ is the risk

aversion factor: it models the risk aversion of the nice users (α >1) leading to earlier collapse of the service than predicted by *d* alone.

In case (c), when hackers are more successful in monetizing the value of nice guys resources than we expect, i.e. $d < 0$, it turns out that the value function has a local maximum at h_2. We interpret this to mean that using illegal means, the hackers manage to obtain value from parties that are not directly engaged in the Internet interactions.

In the expression, β is a positive value, we expect it to be in the range 10…1000. The value of 10 would mean that full collapse of the Internet occurs when some Trojan will infect a benevolent user once in ten interactions of the nice user, and value 1000 that the collapse occurs when the infection rate is one in 1000 interactions.

4.2 Analysis of hacker gains

Hacker gains are $v_h = ht\,|I| = ht(1-\beta^2h^2)I_0$.

Normalizing the gains to average temptation and the size of the set of Interactions when there is no hacking, we obtain: $w_h = h(1-\beta^2h^2)$.

The first derivative is $\frac{dw_h}{dh} = 1 - 3\beta^2h^2$. The derivative is obviously positive for small h, i.e. the gains keep increasing as a function of *h*. The first derivative has a root at: $h = \sqrt{\frac{1}{3}}\frac{1}{\beta} = 0.577*h_{max}$. We interpret this to mean that the brotherhood of hackers can maximize their overall gains when the share of successful hacking interactions is about 57% of h_{max}. (This applies to the case when the decline model works i.e. $0 \le d < \beta$). After this point, the collapse of the service starts eating into hacking profits. For the technically more advanced hackers, it becomes more reasonable to attack the weaker hackers than just keep exploiting the nice hosts.

4.3 Tax of hacking on Internet use

We seek to find an answer to the 3rd question about the split of value between the hackers and the benevolent users. Let us call this share of gains of hacking in the overall welfare, a hacking tax.

When $d > 0$, the hacking tax = $\frac{ht}{1-dh}$. Figure 2 plots the hacking tax for values of *t* and *s*.

Figure 2 plots the hacking tax using the sucker payoff of -5, when the hackers manage to monetize 40% of the value they destroy (Tax1), and the sucker payoff of -10, when the hackers manage to monetize, 15%, 40% or 60% of the value lost by the nice users (Tax2, Tax3, Tax4 respectively).

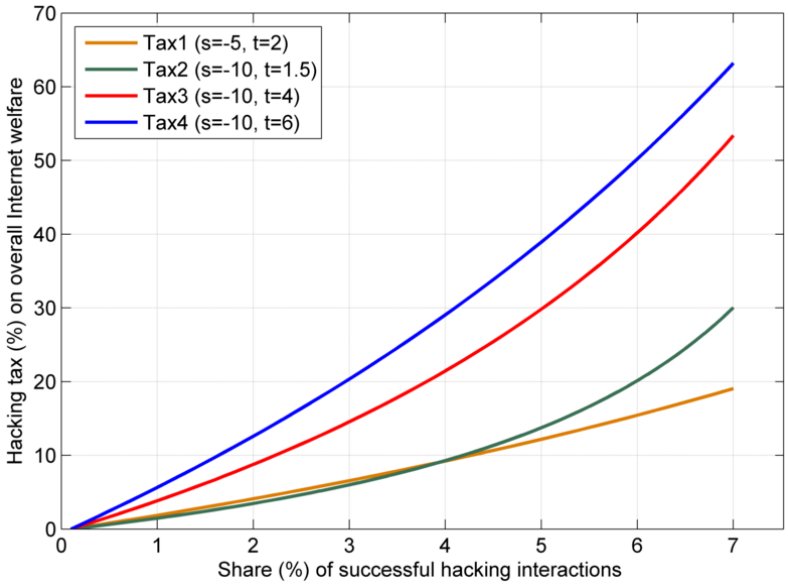

Figure 2. Hacking tax on overall welfare versus the share of hacking interactions (h)

The plot for the sucker payoff of -20 breaks the Internet when the share of successful hacking is around 6%. This is the level of maximum bot penetration [53] observed in some countries without leading to the collapse of Internet in that country. It is reasonable to argue that because of a strong tendency towards risk aversion, typical of consumers e.g. when the hacking tax grows (>20%), the users will become security conscious and will take measures to lessen the likelihood of being hacked. This leads us to believe that the average sucker payoff is likely to be 5 or 10 times the average payoff of two nice users interacting, and that the average temptation is likely to be less than 50% of the average loss caused by hacking. However, the higher payoffs may be possible when the share of hacking stays low and focuses only on high value targets, i.e. industrial espionage.

It is logical that the payoffs depend on factors: (i) whether the majority of Internet users store valuable information on their systems or they use them for entertainment purposes? (ii) what is the security awareness of ordinary users and therefore their willingness to invest in security, and (iii) what strategies hackers decide feasible to pursue: purely opportunistic scavenging of any value using bot rentals, DDoS and spamming; or careful choice of high value targets and treating bots as consumables.

5. Simulation Experiments

We designed a simulation of multi-round prisoner's dilemma game to study the distribution of welfare between Internet users and hackers. The game simulates interactions between nice users and hackers in the Internet, and investigates how sharing the outcome of previously commenced interactions via an Internet-wide reputation system would affect the welfare distribution between both types of players. We refer the resulting Internet as *cooperative-Internet*, and compare the welfare of the Internet users under cooperation with the current Internet. The welfare analysis attempts to reveal if the adoption of an Internet-wide reputation can result in achieving sustainable cooperation in the Internet, such that it contributes to the welfare of Internet users and reduces the hacker's payoff in the long run.

Table 3. Payoff matrices for the simulation

	Nice users	Hacker
Nice host	(1, 1)	(-5, 2)
Hacker	(2, -5)	(0, 0)

(*a*)

Nice users	Hacker
(1, 1)	(-10, 1.5)
(1.5, -10)	(0, 0)

(*b*)

Table 3 defines the payoff matrices for our multi-round prisoner-dilemma game. The gain 1 of an interaction between two normal hosts corresponds to the mean that the hosts continue with the service usage, as they are gaining a positive payoff under normal conditions. The simulation in case (a) assumes that hackers are able to monetize 40% value of the compromised information or the loss of an ordinary user. In case (b) the loss to a nice user is higher, but the capability of the hackers to monetize on the infection is lower: 15%. We use the payoffs in (b) to model the case where an *advanced* hacker successfully takes on a high value target. Due to multi-round nature of the game, in the last element of the matrix, we average the payoff for the case when two hackers *or bots* interact over an ordinary host.

The values in the payoff matrices of Table 3 are inspired from our analysis of hacking tax in Figure 2. The graph for the sucker payoff of 20 broke the Internet for the share of 6% hacking, the maximum in some OECD countries [53]. Whereas, the sucker payoff of 10 and the ability of hackers to monetize 40% or 60% of the compromised value corresponds to hacking tax of 55% and 65% on the overall Internet welfare. This would imply that Internet usage in those countries is already at its lowest, which clearly does not correspond to the reality. Thus, we choose the values of Tax1 and Tax2 in the payoff matrices of Table 3.

We note that the losses caused by hacking are very difficult to assess. For example, how to assess the damage to public image of a company, is a difficult question. For this reason, we have defined the useful limits of our model as $0 \leq d < \beta$. We concluded that the model is not applicable for the case, when the hacking destroys a lot of value $d \geq \beta$ or when hacking is more profitable than we expect $d < 0$. Rather, the intent of the simulation is to reveal that sustainable increase in the Internet welfare is possible due to cooperation.

5.1 Simulation setup

The simulation begins with N hosts and an initial bot-concentration of g%, and runs for a large number of interaction rounds, emulating an infinitely repeated game. The infinitely repeated nature of the game allows to study the evolution of welfare and cooperation among Internet players. An interaction round in the game comprises of a set of interactions between players: hackers or end-users, where an interaction is always between two players. The simulation takes a total of 20% hosts in each interaction round, where g% of these hosts are attackers. These hosts interact with each other and note the other host as either: 1) a benevolent host; or 2) an attacker. The simulation notes the payoffs of each interaction from the corresponding payoff-matrix in Table 3, for the purpose of welfare analysis.

Each interaction round is simultaneously played under the current Internet and the proposed cooperative Internet. The players in the current Internet do not share their learning of interactions with the rest of the population. In contrast, the same players under the cooperative Internet share the learning of their interactions at the end of each interaction round via a trusted reputation system, in an attempt to form a social memory of the Internet. The reputation system leverages these learnings from each interaction round to generate the list of malicious hosts: *blacklists*. For the purpose of this simulation, we set a threshold of

three misbehavior evidences before the reputation system blacklists a host for time 'T_0'. Consequently, the blacklisted host cannot defect any Internet host.

We model a hacker's interaction with a normal host in two ways: 1) it receives the defection gain over the ordinary host; or 2) it fails to infect the host. The latter case may happen due to existing investments of the host in its security, i.e. firewalls, intrusion or virus detection. We define a *bot-infection rate* to model this behavior, such that a hacker receives the defection gain only in the case it successfully infects the victim, which can lead to the birth of a bot. Thus, the bot-infection rate 'p' directly models the *bot-birth process*, i.e. a bot infects the victim with probability 'p'. Consequently, the simulation also bears a model for the *death* of bots. The bots in the Internet generally have a lifetime, and an active bot typically meets its life, when the infected host improves security. To this end, the simulation defines an average lifetime of bots, to reflect the clean-up activity and model the steady bot-penetration of the Internet. However, a bot can expire earlier in the cooperative Internet, if the misbehavior evidences from multiple hosts lead to its *blacklisting* in the reputation system. The user of the host subsequently performs the cleanup activity to regain the Internet access, resulting in death of the bot.

For realistic modeling of the Internet hacking activity, we divide hackers into: 1) master-bots, which focus on zero-day vulnerabilities and thus generate bots for bot-rental business; and 2) scavenger-bots, which hunt for any value they find and are treated as consumables. The master-bots generally operate in a stealthy manner (i.e. by staying below the detection threshold) and thus live a much longer life. They additionally pursue the high-value targets. We use the payoff-matrix (B) for interaction of master-bots with high-value hosts, whereas payoffs in (A) are used for the interaction of scavenger-bots with the ordinary hosts.

The simulation collects payoffs as well as records learning from each interaction round, for the purpose of welfare analysis. The sharing of learning outcomes benefits the players of the cooperative Internet, which is in contrast to the current Internet where the hosts solely rely on their local firewall policies and self-collected evidences. We measure the overall Internet welfare by averaging the sum of all interaction gains with benevolent hosts and the defection losses from hackers, to the total number of interactions. This is shown by the following equation:

$$W_h = \frac{\sum Payoffs}{n} = \frac{\sum Interaction\ gain + \sum Defection\ loss}{n}$$

5.2 Simulation Results

The understanding of the Internet security can vary in different settings; thus affecting the values of the payoff matrix and nature of interactions. We ran our simulation under three different cases of Internet security: a) Normal case, where bots and hosts are equally active in the Internet; b) Bots are more active than normal hosts; and c) Hackers exploit the zero-day vulnerability to create scavenger bots i.e. for bot-rentals. We study the first scenario in detail to answer one of the core questions of this paper, whereas the remaining scenarios are only discussed briefly. The simulation results depict the evolution of welfare and cooperation under different cases of the Internet security.

The first simulation scenario considers the case where Internet bots are as active as normal hosts. Figure 3 presents the normalized Internet welfare against different levels of bot-penetration. The bot-penetration is the share of bots among Internet hosts, and it is varied from 0.5% to 7% in population for each simulation round. The simulation ran for 2000

interaction rounds, of 60 interactions each, on a population of 1000 simulated hosts. The welfare analysis reveals that cooperative-Internet would result in high overall welfare of its hosts. This is because once a bot crosses the detection threshold in the number of observed malicious acts, blacklisting orchestrated by the reputation system protects Internet hosts against any subsequent defection attempts from this bot, contributing to the overall Internet welfare. Thus, hackers experience reduced payoffs from the deployment of an Internet-wide reputation system.

The simulated welfare in Figure 3 corresponds to our modelling of Internet interactions, in particular of Section 4.3. The welfare of current Internet in Figure 3 is nearly at the same level, as the net welfare obtained after deducting the hacking tax in Figure 2. The results from the simulation and our mathematical modelling corroborate, and they independently validate the other method. Under this premise, the net welfare under a different understanding of the interaction payoffs can be sought from Figure 2.

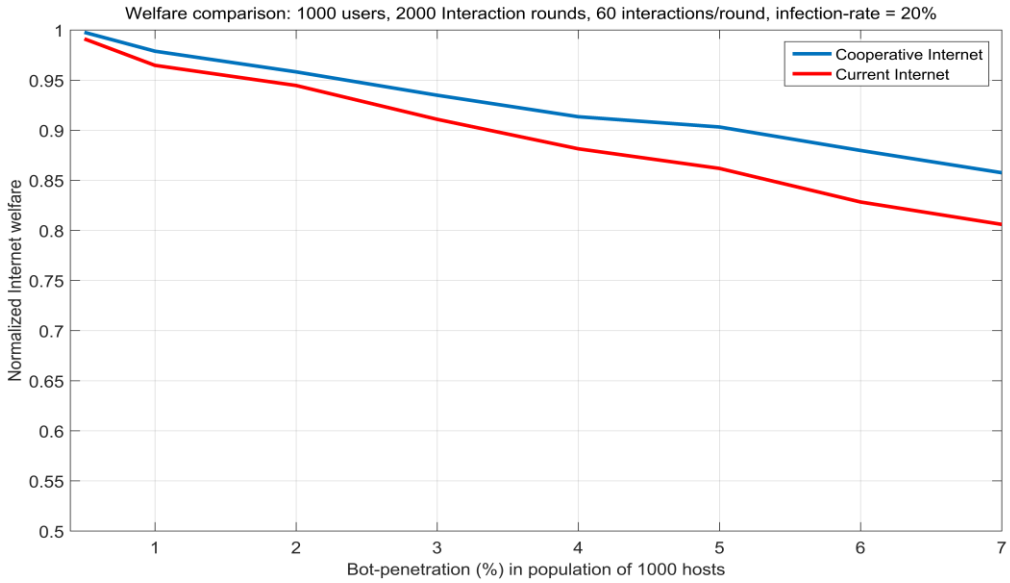

Figure 3. Internet user's welfare analysis versus bot-penetration levels

Figure 4 reveals whether the adoption of an Internet-wide reputation would contribute to achieving sustainable increase in the welfare of Internet users. We study the problem over a population of 1000 simulated hosts, in 2000 interaction rounds of 60 interactions each. The bot-penetration in the population is assumed at 2%, which is the average bot concentration in the OECD countries [53]. Though the welfare fluctuates initially, the figure reveals that the net Internet welfare increases under the cooperative-Internet and eventually emerges as stable. This is due to an additional mechanism of blacklisting the attackers in cooperative Internet via the reputation system, in addition to the existing investments on security in the current Internet. The result supports our claim that achieving cooperation based on the principles of indirect-reciprocity, i.e. via an Internet-wide reputation system is an eventually stable strategy that could improve the Internet welfare.

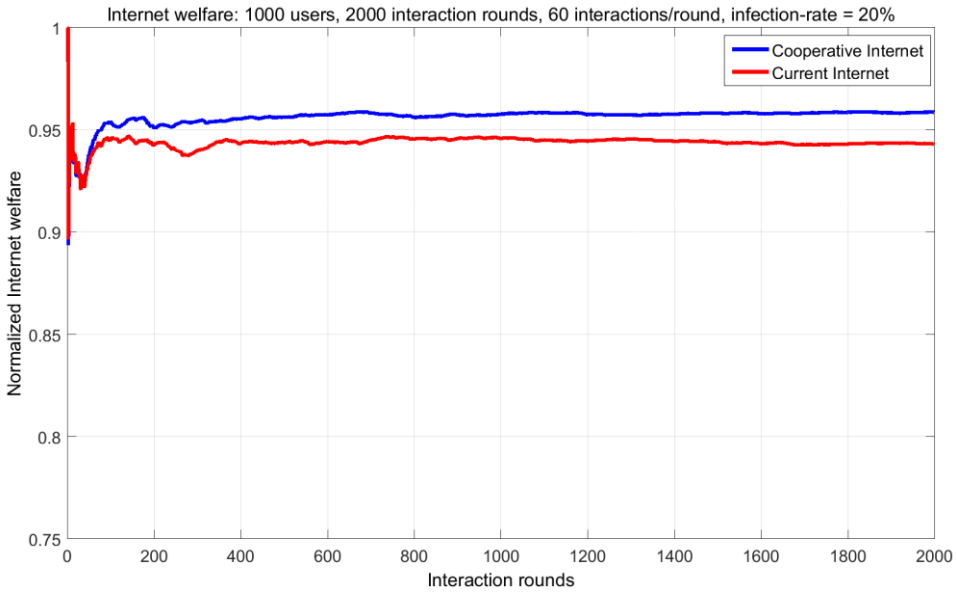

Figure 4. Evolution of the Internet user's welfare (per interaction round)

Figure 5 presents the split of overall Internet welfare between scavenger-bots and master-bots, and how an Internet-wide reputation system impacts this distribution of welfare. Since the master-hackers operate in a stealthy manner (i.e. by staying below the threshold), their welfare remains unaffected. However, the scavenger-bots that are treated as consumables and often as a means for launching attacks, experience reduced payoffs in the cooperative Internet. This is because they meet the detection threshold quickly due to their active nature and thus are blacklisted by the reputation system. The result indicates that introducing the Internet-wide reputation would more seriously impact amateur or mid-level hackers (and their activities) than advanced hackers, and thus contribute to the overall Internet welfare.

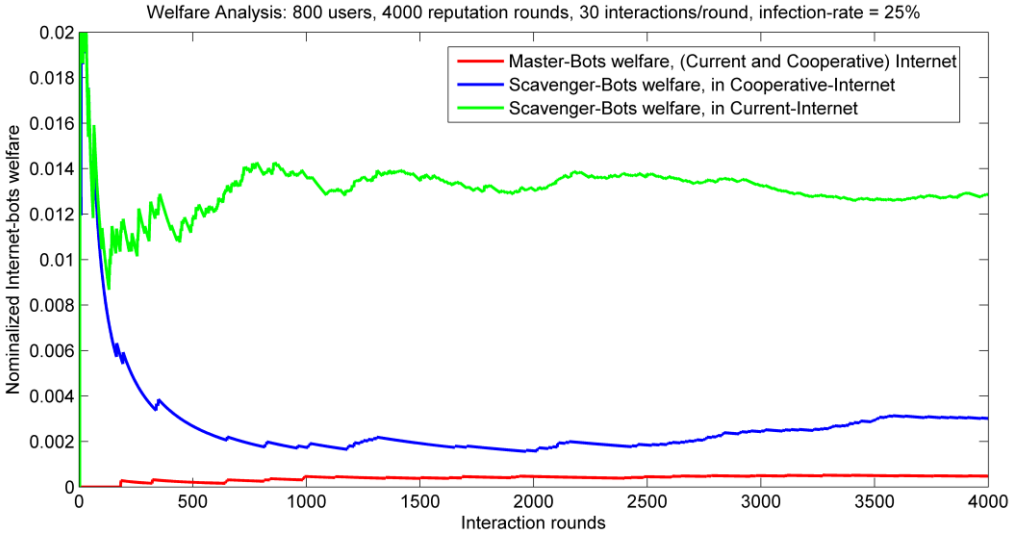

Figure 5. Split of the welfare between Internet bots

5.2.1 More Simulation Scenarios

The simulation results for scenario b) and c) are respectively shown in Figure 6 and 7. Scenario (b) simulates the case where Internet bots are more active than the ordinary hosts, and thus have higher share of hacking interactions. For the purpose of simulation, we consider bots three times more active than the ordinary hosts. As a result, the share of bot-interactions is three times more than the previous scenario, while the rest of the parameters are the same.

Similar to the previous results, the welfare comparison in Figure 6 reveals that cooperative Internet yields high welfare of its users, due to the additional mechanism of evidence sharing compared to the current Internet. However, the net welfare in this case is far lower than the welfare computed for scenario (a). This is due to the high number of bot-interactions, due to more active nature of bots, which causes the net welfare to drop to the level where bot concentration appears thrice of the actual bot-penetration (2%). The welfare outcome of this scenario closely corresponds to the case where bots have high infection rates, and yield high bot-birth rates. Thus, we only refer to that case briefly here.

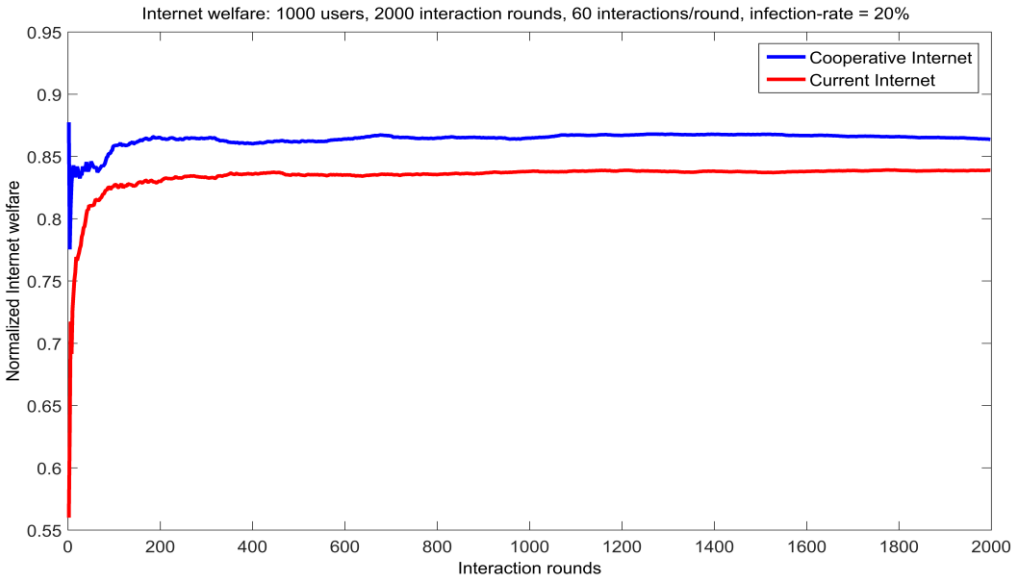

Figure 6. Evolution of the Internet welfare for simulation scenario-2 (active bots)

The scenario (c) simulates the case where master/advanced hackers exploit a zero-day vulnerability, i.e. to create scavenger bots: for bot-rentals and deteriorating Internet security as a whole. In this case, the bot-infection rate at the beginning is high, since vulnerability is still unpatched. During this phase, a large number of hosts are vulnerable and thus infection rate is high. This leads to low welfare in the beginning, as shown in Figure 7. For the purpose of simulation, we assume an initial bot-infection rate of 90% for master-bots and 65% for scavenger bots, i.e. a bot infects an Internet host with these probabilities.

However, as soon as the vulnerability is discovered and patched, the lifetime of the bot in the host ends, and the host is no longer vulnerable to attack. For the same vulnerability, the number of vulnerable Internet hosts decreases, thus reducing the bot-infection rate. However, not all the hosts update their software or patch vulnerabilities in time. In reality, some hosts remain vulnerable. We account such hosts by a relatively lower bot-infection rate. The simulation assigns a bot-infection rate of 40% for master-bots and 20% for scavenger-bots, in the post-vulnerability discovery phase. This also accounts for hosts that simply have poor security, and thus will be vulnerable to some attack type. Nevertheless, the bots created during the post-discovery phase live a much shorter life, since Internet has established procedures to deal with the vulnerability, reducing the bot's lifetime in the infected host.

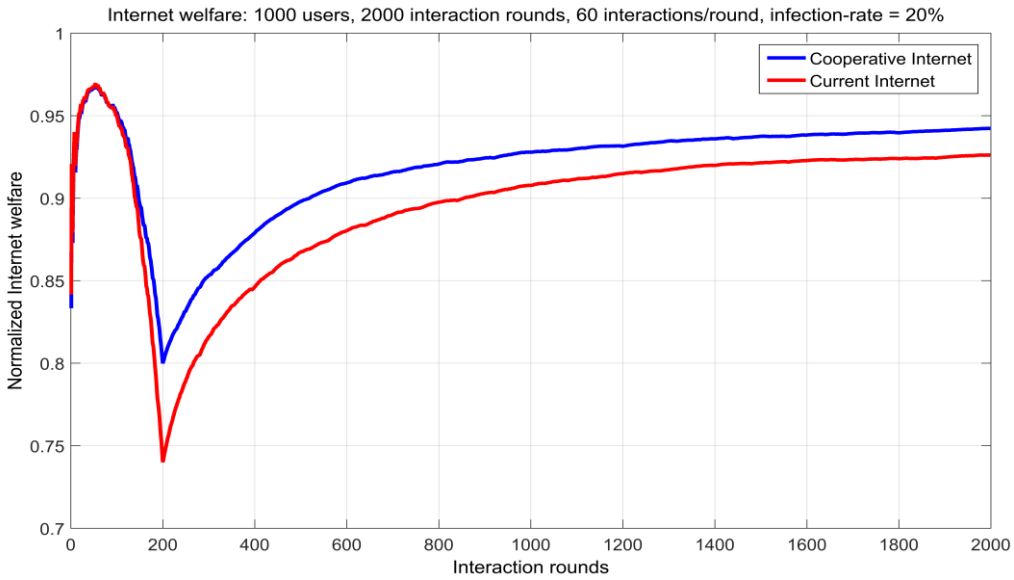

Figure 7. Evolution of the Internet user's welfare for simulation scenario-3

The figure reveals a welfare decline in the beginning of the simulation. This is because the early infections are undetected by the Internet (and its hosts), leading to birth of bots that in turn defect other hosts, causing a monotonous decline in the Internet welfare. The decline however is more severe for the current Internet. In comparison, the cooperative Internet offers much better welfare, even though it does not know about the vulnerability. This is because the blacklisting orchestrated by the evidence sharing filters some of the aggressive bots, thus containing the damage. In the post-vulnerability detection phase, the welfare steadily begins to rise until it emerges nearly stable towards the end of simulation.

For all the simulated cases, the results in general reveal that the cooperative Internet yields higher welfare of its users compared to the current Internet, due to evidence sharing via an Internet-wide reputation system. In particular, the results show that cooperative Internet can contribute to better tackle some of the most typical and advanced internet security cases, such as exploiting of the zero-day vulnerabilities.

5.3 Discussion

The use and development of the Internet is a market driven process: there is very little regulation compared to physical society with its legislature, law enforcement and taxation to fund activities that ensure continuation and sustainability of the cooperation. Compared to organized physical societies, Internet users do little joint efforts to ensure continuation and sustainability of the cooperation. For example, there is practically no taxation that would fund the counter activity to cybercrime. In operational practice, many state-of-the-art security methods are based on self-help, i.e. using only the local knowledge/policies.

5.3.1 State of the art in Internet

This section overviews the state of the art and emerging trends in Internet cooperation, and discusses how a reputation system can contribute to it. Threat intelligence is already one of the emerging trends in the Internet security today. Predictably, the ability to share threat intelligence will be critical to the next generation of the security solutions. Networking community has already made efforts with creation of the frameworks, such as vulnerability databases (i.e. CVE [56]), OpenIOC [57], and CERT coordination centers [8]. These developments aim to improve Internet's responsiveness to threats, by creating frameworks for sharing threat information. However, the traditional methods of processing threat

intelligence are no longer practical, since they require human intervention to encode threat information into firewall rules or written reports. The key in the Internet security today is to automate as much as possible by designing a workflow that automatically detects, responds and contains attacks. This paper briefly presents our approach that seeks to make an effort towards automating the process of detecting, sharing and leveraging the threat intelligence to improve Internet security.

OpenIOC (Open Indicators of Compromise) is one such format for recording, defining and sharing the threat information in a machine-digestible format, minimizing the need for human intervention. Similarly, vulnerability databases aim to provide a baseline for sharing security vulnerabilities. For example, CVE (Common Vulnerabilities and Exposures) is an industry standard for sharing common names of publicly known vulnerabilities, between security products and services [58]. The underlying idea is to ease the sharing of threat intelligence across different networks, security tools, and to provide a baseline for security solutions. Similarly, the regulators in different countries are mandating security incident reporting with CERT-CC. The CERT (Computer Emergency Response Team) cooperation responsibility applies to all major ISPs at national/regional level and provides an overview of the emerging threats. Software vendors and governments leverage CERTs to address software vulnerabilities and secure the national infrastructures, respectively.

A wide range of state-of-the-art security solutions are based on self-help, particularly in legacy networks. Security vendors are now increasingly adopting the sharing of threat intelligence in their solutions. We can broadly categorize these solutions into: application-based, host-based and network-based solutions.

The host-based solutions typically employ a firewall on end-systems and leverage cloud computing to process threat intelligence from firewalls on Internet hosts, around the world. The cloud processing provides the security vendors with a global view of emerging threats and thus enhance preparedness [59]. Typically, threat recognition leverages vulnerability databases as well as searching of attack signatures in the processed traffic. The use of cloud computing offers advantages in terms of saving end-system computing resources, storage, provides the global threat overview, and thus quicker threat mitigation. But, for mobile networks, the use of host-based approach has several downsides, because it allows unwanted traffic to travel all the way to mobile device which: a) clutters the radio interface; b) impacts bandwidth availability of network for legitimate users and network operations; and c) disturbs sleep cycle of resource-constrained battery powered terminals. The same applies to cloud-based security solutions for services running on the end-hosts. These cloud-based security solutions are mostly optimized for service-oriented threats only and do not necessarily address the end-system security challenges.

In comparison, for 5G, where many of the new end devices can be too weak or resource constrained to run host-based solutions, a network-based approach to security has obvious advantages. It can additionally contribute to radio spectrum efficiency by filtering unwanted traffic in the network, and thus ensure availability of radio resources for legitimate needs. Besides leveraging cloud computing for filtering attacks in the processed traffic, network-based solutions (such as Customer Edge Switching) can overcome the inherent Internet weaknesses, such as source address spoofing, traffic floods, possibility of network scans, botnets and DoS, at the level of interaction between networks. Hackers often direct these attacks to raise availability concerns and disruption of legitimate services. If not mitigated by the network, these malicious flows can reach end-hosts, and in addition to damages can disturb the sleep cycle of the battery powered terminals, and thus deplete the battery. Thus, we argue that deploying cooperative security among the networks is more rewarding and has obvious advantages for the Internet and in particular for 5G.

5.3.2 Evolution of state-of-the-art towards Cooperation

This section discusses the state-of-the-art in modern ISPs and how it can evolve to achieve cooperation in the Internet. The state of the art in some advanced ISPs is such that they are able to trigger additional monitoring upon observing communication with known malicious hosts or subnets. If the monitoring reveals that the ISP has an infected host in its network, rather than blocking the host, the ISP will automatically contain the harm by reconfiguring the infected machine into a sandbox-style access to the Internet. This allows the host to update its security software in order to get cleaned, and prevents from causing harm to other Internet hosts. The approach does not assume that the attacker's network is cooperative.

ISPs generally log all the IPs assigned by its DHCP to the hosts. Hence, upon processing attack evidence that reveals an IP address, the ISPs can generally trace the host. Similarly, all the NAT bindings for a host behind NAT must be logged. Under ubiquitous NATting of all communications, a separate Host-ID that is more stable than a NAT binding can reduce the amount of required logging.

Next, we discuss how state of the art can evolve to achieve sustainable cooperation in the Internet, and where some network entities can have an essential role. From a technical perspective, under the assumption of a random bot location in the Internet and cooperative network administrators, solving the problem of sustainable cooperation requires: (a) a system of stable identities [54]. Hosts cannot self-adopt the identities that are easy to link with network and application layer events. This is even true for IP addresses that act as identifiers. A trustworthy and responsible entity must assign these identities, for example, mobile operators can leverage their infrastructure to provide such identities. To link the evidence of misbehavior with containing a bot, (b) a chain of trust from the victim to the network serving the bot is required. Since most hosts are wireless and battery powered, (c) an efficient security solution should block most of the unwanted traffic in the network, before it reaches the battery-powered device, and disturbs the sleep cycle of device and clutters the air interface. This is also in-accordance with the 5G requirements for longer battery lifetimes of wireless devices [55]. Finally, when a Trojan has infected a host, (d) the network administrator must take action to contain the bot in the network. Such containment is an action under *Rule 4*.

The problem of establishing cooperation applies to the use of communication capacity, as well as to the use of the resources and information on the end-systems. One can seek better network service or launch DoS by hogging more than the fair share of network resources. Moreover, by non-authorized use of the resources and information stored on the end-system, it is possible to gain huge benefits.

Internet has practiced the paradigm of finding vulnerabilities, learning their exploits and patching the weaknesses for long now. Cooperation offers a strategic shift in security, and focuses on containing the harm at the earliest and discouraging the hosts from choosing a defecting strategy in the first place. In comparison to the traditional security, which allows malicious traffic to traverse all the way to the destination where it could or could not be filtered, our approach aims to filter the malicious traffic as early as possible and as close to the source as possible, due to the cooperation of networks. Such a cooperation supervised by an Internet-wide reputation would motivate the *non-cooperative* networks that forward the malicious traffic, to improve their security, ensure security compliance of hosts and thus forward legitimate traffic only, or otherwise they would earn a bad reputation.

The security solutions in state of the art (even the solutions that aggregate the threat intelligence) generally protect only the served entity, which otherwise would receive the Internet attacks. However, in addition to this classical *receiver-oriented* security, we stress to locate the misbehaving hosts and networks that originate the malicious traffic and form (and distribute) the reputation of hosts or networks that do not take corrective actions, and hence keep forwarding the malicious traffic. The rest of the networks can reflect this reputation in their local security policies, for example to restrict access from ill-behaving sources, and thus ensure network availability for legitimate uses. A (cooperative) network shall process the misbehavior evidences aggregated under one of its hosts to restrict the access of malicious host, and execute steps to ensure its cooperative behavior. This in effect shifts the responsibility of filtering malicious floods from receiver to the sender network. By dynamically updating the list of malicious sources: hosts and networks, the reputation system can help security solutions to keep up with dynamic adversaries, i.e. hackers.

The use of ubiquitous evidence collection and reputation would potentially shorten the lifetime of bots, limit the scope of defecting strategies, and the type of activities that are worth programming into the exploits, affecting the bot-rental business that programs these activities. This will more severely affect amateur and mid-level hackers that rent these bots to target normal users or vulnerable networks, as shown by the simulation experiments as well.

Based on this analysis, we predict that cooperation will change the security warfare in the resulting Internet, such that the general Internet users will be better off. Besides deciding to pursue the traditional security warfare, hackers in the cooperative Internet could: (a) attack the reputation system to discredit it; or (b) target zero-day vulnerabilities to exploit their victims or to create botnets. We have studied the question of system attacks on robustness of the Internet-wide reputation system in [10-12], and have analyzed the scope of traditional warfare previously. Thus, we predict that the paradigm of Internet attacks will shift from hackers targeting users in the current Internet to more *advanced* hackers (that are capable of) targeting zero-day vulnerabilities on (high value) targets, i.e. to create botnets or to receive payoffs in the resulting Internet. As a result, general users will be better off, since: a) amateur/intermediate level hackers that rely on the classical Internet weaknesses or on bot-rentals will suffer from deployment of the Internet-wide reputation; and 2) the advanced hackers will preferably focus on high value targets, without being too active to cross the detection threshold for being blacklisted.

The reputation system can offer advantages over state of the art, for example in handling attacks on zero-day vulnerabilities, where classical methods such as vulnerability databases would fail to contribute. In comparison, the reputation system could contain the damage by demoting the reputation of hosts or networks that frequently originate malicious traffic, and thus limit the extent of exploitation of zero-day vulnerabilities. Taking a step further, the misbehavior evidences aggregated against a host identity shall cause the network of the host to restrict the host's access (for example, to well-known public Internet domains only, such as Google etc.). This shall prevent a malicious host from exploiting zero-day vulnerabilities on weak Internet hosts that typically reside in the private Internet domains, and thus affect the bot-rental business that thrives by exploiting such vulnerabilities on legacy hosts and less security aware users. Similarly, the reputation system could contribute to the security of new/emerging services, where vulnerability databases have little to contribute initially.

6. Implementing Internet-wide trust management

We expect that it will be much easier to foster cooperation among some 1800 ISPs that

have numerous business relations rather than trying to guide the behavior of more than 3,5 billion hosts. Being in the business relations with other ISPs, their interactions are un-ending, as required by *Rule 1*. ISPs work under market conditions, so there is no reason to believe that they would not be capable of learning required for *Rule 1* to apply, provided that they are able to earn from investments they make to security. Unlike hosts, ISPs cannot as easily just disappear or hide their identity. Having a stable identity and continued presence as a public service provider, it is difficult for an ISP to defect under *Rule 2*. Most ISPs are inclined to cooperate unless coerced by governments or powerful criminals to act otherwise. There are known cases where spammers created their own ISP – this is an exception among ISPs, similar to there being some criminals among people while most of us abide by the law. Thus, we observe that conditions exist for cooperation to become the dominant strategy among ISPs.

Based on this reasoning and referring to the results of game theory on the conditions that must be met for a cooperative strategy to become dominant, we propose that *each ISP and large customer network must accept responsibility for the cooperative behavior of the hosts that it serves*. A customer network is a stub network (in terms of Internet routing) that provides Internet connectivity to a number of hosts but does not carry any transit traffic. The responsibility for the hosts implies that the ISPs (and administrators of the large customer networks) agree to cooperate in order to root out malicious behavior of their hosts.

For ISPs, this is the de-facto situation already today in many countries with advanced Internet security, for example Finland. The law on consumer rights justifies the need for the ISP's responsibility. However, in state of the art, the responsibility of ISPs (e.g. in Finland) is limited to the case when an infected host in the ISP network can cause harm to the network. This limitation is dictated by the privacy of communications, i.e. network traffic monitoring is only allowed for security reasons when the purpose is to protect the network. Another reason for de-motivation towards a more active role of the ISPs lies in the difficulty of the ISPs to earn revenue from better security to the end systems.

Currently the regulators in many countries mandate that ISPs participate in security incident reporting with CERT [8], while other businesses are so far exempted from such obligation – they may however cooperate voluntarily. The CERT cooperation responsibility can be extended to major private customer networks. Indeed, in 2017 EU is planning to approve a Directive that will broaden the security incident reporting to many actors that are seen as part of the critical infrastructure of the member countries. The CERT cooperation obligation provides necessary basis for the sharing of misbehavior evidences among Internet entities and thus for establishing a reputation system.

We assume that it is very unlikely for all ISPs to simply trust each other, to start exchanging attack evidence, even in an aggregated form. It will be easier to initiate the development of the cooperative Internet, which makes use of the reputation of customer networks and hosts, from trust domains. A trust domain may include networks under one ISP, one mobile operator or the networks of most ISPs that have operations in a single country. If the deployment is not feasible under a market driven process, it is possible for the regulators to set new rules for the operations, similar to CERT cooperation obligation.

6.1 Trust oriented approach to network security

The cooperative Internet will benefit from a particular approach towards security. It aims to employ all possible means for detecting attacks, identifying the hosts used by hackers, and

collecting evidence from every host, connected device and ISP. The evidences are passed to a trusted aggregation service that will produce indications for trusted network-based monitoring. Network monitoring can validate the evidences in the served traffic and report to a reputation system that generates dynamic grey and black-lists of networks and hosts, and distributes them to network-based firewalls. It is important that a trusted network-based system is employed to validate the attack evidences from end-hosts. Otherwise, it leaves a window of opportunity for botnets to generate false evidences against innocent hosts, leading to denial of service on the victims and loss of faith in the reputation system.

Towards that end, we propose a cloud-based firewall namely *Customer Edge Switching* (CES) [17-24] that would make the hosts cooperative in nature. It follows the firewalling model of mobile broadband networks, where mobile hosts are behind a network-based firewall. We propose CES as a means of connecting customer networks to the global Internet. CES is an extension to Network Address Translators (NAT), and it can operate as a cooperative firewall that manages all the communications by policy. Policies can be defined for ISPs, hosts, subnets, users or applications. Policies can be either static or dynamic. A dynamic policy reacts differently to each sender depending on what the edge node knows about the remote network/host/user and depending on the security situation faced by the network.

The adoption of CES does not require changes to end-hosts. To this end, a customer edge switch can be complemented with a realm gateway (RG) [19-22], which allows dynamic and unilateral initiation of communication by legacy Internet hosts to the servers located in the private networks. The behavior of CES for outbound connections to legacy hosts is the same as NAT. Due to RG capability, CES can be deployed one network at a time fulfilling the need of incremental deployment. We have implemented our solution using Software Defined Networking concepts, i.e. adhering to the Control and User plane split architecture, which is one of the key technologies for 5G. In [24], we discussed detailed contribution and application of CES/RG approach to 5G mobile networks; which is our key for facilitating cooperation between customer networks. CES can contribute to meet the energy challenge of 5G [55]: facilitating longer battery lifetimes for wireless devices, such as mobile-hosts or sensors, by allowing them to sleep as long as possible [20]. This is because the hosts in the private realm will have an improved network-based firewall, which can filter the malicious flows before they reach the end devices, and because hosts are only reachable via a policy.

We have implemented a demonstrator of the Customer Edge Switch on Linux and have made it available for the community at [17]. CES is designed to collect all the evidences and pass them on for trust processing. CES makes the basic act of communication *receiver-friendly*, establishes identities for the hosts, and contributes to eliminate address spoofing and distributed denial of service attacks. CES facilitates identifying the customer networks involved in communication. Once the identification is in place, it contributes to collect the information on behavior of the entities involved in communication and start forming a coherent opinion, i.e. on the reputation of the Internet entities.

7. Conclusions and Research Challenges

In this paper, we have addressed the question whether adopting better means of cooperation i.e. via an Internet-wide reputation system can potentially increase the welfare of Internet users and reduce the hacker's payoffs. The paper reveals that there is an added value in the Internet that can be gained by introducing the proposed trust management in the Internet.

The paper suggests that on the evolution path of the Internet, it is time to look for smarter

and faster 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. In the paper, we model the welfare of Internet users as a function of hacking activity in the Internet and after introducing an Internet-wide reputation system. We study the impact of deploying the reputation system on the welfare of Internet, hacker's payoff, and whether it leads to achieving sustainable Internet cooperation.

For the purpose of implementing such a reputation system in the Internet, we propose (A) Customer Edge Switching that operates as a cooperative firewall and (B) an Internet-wide trust management [12]. The Internet-wide trust management mimics our collective opinion or social memory of other's behavior. This draws on the human competences of using language to describe a behavior, gossip about it and prune behavior that is deemed anti-social by the majority. These traits have made humans super cooperators. We claim that it is possible to draw on this social experience and to an extent mimic it in network-based software. This however requires addressing concerns, such as protecting the privacy of communication under global trust management [12], and opens the research topic of trust economics.

Market driven adoption of the proposed solution can be expected if it adds revenue to the Internet ecosystem or reduces costs for the participants. Fresh revenue may come from new services or additional value perceived by the end users, whereas cost reduction can come from automation. In particular, tracing and containing bots from causing harm should be as automatic as possible. If markets fail to lead to an improved level of cooperation among the Internet hosts, alternative is to use regulation to oblige all significant networks to participate in security incident reporting and bot containment, justifying the regulation by common good. We argue that in 5G the motivation for cooperation lies in the provision of ultra-reliable services and ubiquitous access, which is not possible if inherently un-predicable attacks against legitimate services are possible and even easy to execute. Both legal and technical aspects of such cooperation are topics for research.

This paper shows that it is both desirable and feasible to introduce the cooperation among Internet hosts and that this will lead to a sustainable increase in the Internet welfare. We argue that this can be achieved through a set of network-based systems and a certain role of ISPs. The role of ISPs is essential as we argue that it is not possible to achieve cooperation or the same level of Internet welfare based on an end-to-end approach that solely relies on the end-hosts.

References

[1] ITU-T, Global ICT developments, 2016: http://www.itu.int/en/ITU-D/Statistics/, referred 11.10.2016.
[2] "Looking Ahead to 5G," Nokia Networks Whitepaper.
[3] "5G: A Technology Vision," Huawei White paper, 2014
[4] J. H. Saltzer, D. P. Reed, and D. D. Clark, "End to end arguments in system design," in ACM Transaction on Computer Systems (TOCS), New York, 1984, pp. 277-288.
[5] "State of Mobile App Security [Special Focus on Financial, Retail/Merchant and Healthcare]," Arxan, Research Report Volume 3, 2014.
[6] "State of Software Security," Veracode, Security Report Volume 6, 2015
[7] "2014 Cisco Annual Security Report," CISCO, 2014
[8] CERT cooperation and its further facilitation by relevant stakeholders, ENISA, Deliverable WP2006/5.1 (CERT-D3)
[9] J. von Neumann and O. Morgenstern, "Theory of Games and Economic Behavior", Princeton University Press, 1944.
[10] Z. Yan, R. Kantola, Y. Shen, Unwanted Traffic Control via Global Trust Management, IEEE TrustCom2011, Changsha, China.
[11] Z. Yan, R. Kantola, Y. Shen, Unwanted Traffic Control via Hybrid Trust Management, IEEE TrustCom, Liverpool, UK, June. 2012.
[12] L.F. Zhang, Z. Yan, R. Kantola, "Privacy-Preserving Trust Management for Unwanted Traffic Control", Future Generation Computer Systems, 2016.
[13] Z. Yan, R. Kantola, Y. Shen, A Generic Solution for Unwanted Traffic Control through Trust Management, New Review of Hypermedia and Multimedia, Vol. 20, Issue 1, pp. 25-51, 2014.

[14] Y.Shen, Z. Yan, R. Kantola, Game Theoretical Analysis of the Acceptance of Global Trust Management for Unwanted Traffic Control, in Proc. of IEEE HPCC 2013, Zhangjiajie, China, Nov. 2013.
[15] "SRX Series AS Gi/SGi Firewall for Mobile Network Infrastructure Protection," Juniper Networks, Whitepaper
[16] ”5G security,” Ericsson Whitepaper, June, 2015
[17] R. Kantola, Routing Edge to Edge and through Ethernets, www.re2ee.org.
[18] 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.
[19] P. Leppäaho. N. Beijar, R. Kantola, J. Llorente Santos. Traversal of the Customer Edge with NAT-unfriendly Protocols, ICC 2013.
[20] J. Llorente Santos, R. Kantola, N. Beijar, P. Leppäaho. Implementing NAT Traversal with Private Realm Gateway, ICC 2013.
[21] J. Llorente and R. Kantola, "Transition to IPv6 with Realm Gateway 64," IEEE International Conference on Communications (ICC), London, June, 2015.
[22] H. Kabir, R. Kantola, J. Llorente Santos, Security Mechanisms for a Cooperative Firewall, CSS 2014, Paris 2014.
[23] H. Kabir, J. Llorente Santos, R. Kantola, Securing the Private Realm Gateway, IFIP Networking 2016, Vienna 2016.
[24] R. Kantola, J. L. Santos, and N. Beijar, "Policy based Communications for 5G Mobile with Customer Edge Switching," Security and Communication Networks, 2015.
[25] A. Holt, "Prisoners, chickens, volunteers, free riders and suckers: dilemmas on the Internet," in Engineering Science and Education Journal, 1997, pp. 73-77.
[26] R. Axelrod, The Evolution of Cooperation, Basic Books, revised version, 2006.
[27] M. A. Nowak, Why we help, American Scientist, 7/2012.
[28] S. Bowlers, Microeconomics: Behavior, Institution, and Evolution. Princeton University Press, Jan. 2009.
[29] C. H. Papadimitriou, "Algorithms, Games, and the Internet," in Proceedings of the thirty-third annual ACM symposium on Theory of computing, Newyork, 2001, pp. 749-753.
[30] Ö. Gürerk, B. Irlenbusch, and B. Rockenbach, "The Competitive Advantage of Sanctioning Institutions," vol. 312, pp. 108-111, Apr. 2006.
[31] S. Shivshankar and A. Jamalipour, "An Evolutionary Game Theory Based Approach for Cooperation in VANETs Under Different Network Conditions," submitted to IEEE Transactions on Vehicular Technology.
[32] H. Raiffa. Decision Analysis: Introductory Lectures on Choices under Uncertainty. Addison Wesley, Reading, MA., 1968
[33] Bicchieri, Cristina, “Rationality and Game Theory”, in The Handbook of Rationality, The Oxford Reference Library of Philosophy, Oxford University Press 2003.
[34] Wang, X., Zheng, W., Lu, Z., Wen, X. and Li, W. (2014), Dense femtocell networks power self-optimization: an exact potential game approach. Int. J. Commun. Syst.. doi: 10.1002/dac.2788
[35] I. A. Shah, S. Jan, I. Khan and S. Qamar, An Overview of Game Theory and its Applications in Communication Networks, International Journal of Multidisciplinary Sciences and Engineering, Vol. 3, No. 4, April 2012
[36] S. Floyd and K. Fall, "Promoting the use of end-to-end congestion control in the Internet," IEEE/ACM Transactions on Networking (TON), vol. 7, pp. 458-472, 1999.
[37] T. Alpcan and T. Basar, “A Globally Stable Adaptive Congestion Control Scheme for Internet-Style Networks with Delay”, IEEE/ACM Trans. On Networking, vol. 13, pp. 1261–1274, Dec. 2005.
[38] Jia Y., Zhang Z., Tan X., and Liu X. (2015), Asymmetric active cooperation strategy in spectrum sharing game with imperfect information, Int. J. Commun. Syst., 28, 414–425, doi: 10.1002/dac.2667
[39] Sankardas Roy, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Vivek Shandilya, Qishi Wu, "A Survey of Game Theory as Applied to Network Security", HICSS, 2010, 2014 47th Hawaii International Conference on System Sciences, 2014 47th Hawaii International Conference on System Sciences 2010, pp. 1-10, doi:10.1109/HICSS.2010.35
[40] T. Alpcan and T. Basar. A game theoretic analysis of intrusion detection in access control systems, in Proceeding of the 43rd IEEE Conference on Decision and Control, pp 1568-1573.
[41] T Alpcan and T Basar, A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection, Proceeding of the 42nd IEEE Conference on Decision and Control, pp 2595-2600.
[42] Huseyin Cavusoglu , Srinivasan Raghunathan , Wei Yue, Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment, Journal of Management Information Systems, v.25 n.2, p.281-304, Number 2 / Fall 2008
[43] Simon Parsons , Michael Wooldridge, Game Theory and Decision Theory in Multi-Agent Systems, Autonomous Agents and Multi-Agent Systems, v.5 n.3, p.243-254, September 2002
[44] Assane Gueye "A Game Theoretical Approach to Communication Security" (2011), Electrical Engineering and Computer Sciences University of California at Berkeley. Technical Report No. UCB/EECS-2011-19.
[45] B. Benmammar and F. Krief, "Game theory applications in wireless networks: A survey," in 13th International Conference on Software Engineering, Parallel and Distributed Systems (SEPADS '14), Gdansk, 2014.
[46] M. Nowak and K. Sigmund, "A strategy of winstay loseshift that out performs titfortat in the Prisoners Dilemma game," 1993.
[47] Nowak MA. Five rules for the evolution of cooperation. Science (New York, N.y). 2006;314(5805):1560-1563. doi:10.1126/science.1133755.
[48] Qishi Wu , Sajjan Shiva , Sankardas Roy , Charles Ellis , Vivek Datla, On modeling and simulation of game theory-based defense mechanisms against DoS and DDoS attacks, Proceedings of the 2010 Spring Simulation Multiconference, April 11-15, 2010, Orlando, Florida [doi>10.1145/1878537.1878703]
[49] Salih Y. K., Hang See O., Ibrahim R. W., Yussof S. and Iqbal A. (2015), A novel noncooperative game competing model using generalized simple additive weighting method to perform network selection in heterogeneous wireless networks, Int. J. Commun. Syst., 28, pages 1112–1125, doi: 10.1002/dac.2747
[50] Wang, X., Zheng, W., Lu, Z., Wen, X. and Li, W. (2014), Dense femtocell networks power self-optimization: an exact potential game approach. Int. J. Commun. Syst.. doi: 10.1002/dac.2788
[51] Peng, M., Zhang, Q. and Wang, W. (2008), A utility-based capacity optimization framework for achieving cooperative diversity in the hierarchical converged heterogeneous wireless networks. Int. J. Commun. Syst., 21: 1285–1306. doi: 10.1002/dac.951
[52] David G. Andersen , Hari Balakrishnan , Nick Feamster , Teemu Koponen , Daekyeong Moon , Scott Shenker, Accountable internet protocol (aip), Proceedings of the ACM SIGCOMM 2008 conference on Data communication, August 17-22, 2008, Seattle, WA, USA, doi>10.1145/1402958.1402997
[53] Broadband Portal: http://www.oecd.org/sti/broadbandandtelecom/oecdbroadbandportal.htm, referred 07.09.2014.
[54] P. Kollock, "The economies of online cooperation: gifts and public goods in cyberspace," in Communities in Cyber Space, M. A. Smith and P. Kollock, Eds. Routledge; 1 edition (December 2, 1999), 1999, pp. 220-242.
[55] "5G SYSTEMS," Ericsson White paper, 2015.
[56] “Common Vulnerabilities and Exposures” [Online]. Available: https://cve.mitre.org/index.html. [Accessed on 10.06.2016]
[57] ”OpenIOC,” [Online]. Available: http://www.openioc.org/. [Accessed on 10.06.2016]

[58] "Vulnerability Protection" [Online]. Available: https://www.f-secure.com/en/web/labs_global/0-day-fixes, [Accessed on 10.06.2016]
[59] ”F-Secure Security Cloud, Purpose, functions and benefits,” F-Secure, Whitepaper, 2015