# Coordination in Network Security Games

Marc Lelarge
INRIA - ENS
Paris, France
Email: marc.lelarge@ens.fr

***Abstract*—Malicious softwares or malwares for short have become a major security threat. While originating in criminal behavior, their impact are also influenced by the decisions of legitimate end users. Getting agents in the Internet, and in networks in general, to invest in and deploy security features and protocols is a challenge, in particular because of economic reasons arising from the presence of network externalities.**

**An unexplored direction of this challenge consists in understanding how to align the incentives of the agents of a large network towards a better security. This paper addresses this new line of research. We start with an economic model for a single agent, that determines the optimal amount to invest in protection. The model takes into account the vulnerability of the agent to a security breach and the potential loss if a security breach occurs. We derive conditions on the quality of the protection to ensure that the optimal amount spent on security is an increasing function of the agent's vulnerability and potential loss. We also show that for a large class of risks, only a small fraction of the expected loss should be invested.**

**Building on these results, we study a network of interconnected agents subject to epidemic risks. We derive conditions to ensure that the incentives of all agents are aligned towards a better security. When agents are strategic, we show that security investments are always socially inefficient due to the network externalities. Moreover if our conditions are not satisfied, incentives can be aligned towards a lower security leading to an equilibrium with a very high price of anarchy.**

## I. Introduction

Negligent users who do not protect their computer by regularly updating their antivirus software and operating system are clearly putting their own computers at risk. But such users, by connecting to the network a computer which may become a host from which viruses can spread, also put (a potentially large number of) computers on the network at risk [1]. This describes a common situation in the Internet and in enterprise networks, in which users and computers on the network face *epidemic risks*. Epidemic risks are risks which depend on the behavior of other entities in the network, such as whether or not those entities invest in security solutions to minimize their likelihood of being infected. Our goal in this paper is to start an unexplored research direction consisting in understanding how to align the incentives of the agents of a large network towards a better security.

Our work is a first step in a better understanding of economic network effects: there is a *total effect* if one agent's adoption of a protection benefits other adopters and there is a *marginal effect* if it increases others' incentives to adopt it [2]. In communication networks, the presence of the total effect has been the focus of various recent works starting with Varian's work [3]. When an agent protects itself, it benefits not only to those who are protected but to the whole network. Indeed there is also an incentive to free-ride the total effect. Those who invest in self-protection incur some cost and in return receive some individual benefit through the reduced individual expected loss. But part of the benefit is public: the reduced indirect risk in the economy from which everybody else benefits. As a result, the agents invest too little in self-protection relative to the socially efficient level.

In this paper, we focus on the marginal effect and our work is a first step to understand the mechanism of incentives in a large network. To do so, we need to start with an economic model for a single agent that determines the optimal amount to invest in protection. We follow the approach proposed by Gordon and Loeb in [4]. They found that the optimal expenditures for protection of an agent do not always increase with increases in the vulnerability of the agent. Crucial to their analysis is the security breach probability function which relates the security investment and the vulnerability of the agent with the probability of a security breach after protection. This function can be seen as a proxy for the quality of the security protection. Our first main result gives sufficient conditions on this function to ensure that the optimal expenditures for protection always increase with increases in the vulnerability of the agent (this sensitivity analysis is called *monotone comparative statics* in economics). From an economic perspective, these conditions will ensure that all agents with sufficiently large vulnerability value the protection enough to invest in it. We also extend a result of [4] and show (Theorem 1) that if the security breach probability function is log-convex in the investment, then a *risk-neutral*[1] agent never invests more than 37% of the expected loss.

Building on these results, we study a network of interconnected agents subject to epidemic risks. We model the effect of the network through a parameter $\gamma$ describing the information available to the agent and capturing the security state of the network. In particular, we diverge form most of the literature on security games and relax the complete information assumption. In our model only global statistics are publicly available and agents do not disclose any information concerning their security strategy. We show that our general framework extends previous work [5], [6] and allows to consider a security breach probability function depending on the parameter $\gamma$. Our third

[1] i.e an agent indifferent to investments that have the same expected value: such an agent will have no preference between i) a bet of either 100$ or nothing, both with a probability of 50% and ii) receiving 50$ with certainty

main result gives sufficient conditions on this function to ensure that the optimal protection investment always increases with an increase in the security state of the network.

This property will be crucial in our last analysis: we use our model of interconnected agent in a game theoretic setting where agents anticipate the effect of their actions on the security level of the network. We show how the monotonicities (or the lack of monotonicities) impact the equilibrium of the security game. In particular, coordination among the agents can be ensured only if optimal protection investment increases with the security state of the network. Moreover, we distinguish two parts in the network externalities that we call public and private. Both types of externalities are positive since any additional agent investing in security will increase the security level of the whole network. However, the effect of this additional agent will be different for an agent who did not invest in security from an agent who already did invest in security. The public externalities correspond to the network effect on insecure agents while the private externalities correspond to the network effect on secure agents. As a result of this separation of externalities, some counter-intuitive phenomena can occur: there are situations where the incentive to invest in protection decreases as the fraction of the population investing in protection increases, resulting in a coordination problem. We also show that in the security game, security investments are always inefficient due to the network externalities. This raises the question whether economic tools like insurance [7], [8], [9] could be used to lower the social inefficiency of the game[2]?

The rest of the paper is organized as follows. In Section II, the optimal security investment for a single agent is analyzed. In Section III, we extend it to an interconnected agent and show it connects with the epidemic risk model. Finally in Section IV, we consider the case where agents are strategic. We introduce the notion of fulfilled expectations equilibrium and show our main game theoretic results. We refer to the full version of this work [10] (available on the webpage of the author) for proofs and additional results.

## II. Optimal security investment for a single agent

In this section, we present a simple one-period model of an agent contemplating the provision of additional security to protect a given information set introduced by Gordon and Loeb in [4]. In one-period economic models, all decisions and outcomes occur in a simultaneous instant. Thus dynamic aspects are not considered.

### A. Economic model of Gordon and Loeb

The model is characterized by two parameters $\ell$ and $v$ (also Gordon and Loeb used a bit more involved notation). The parameter $\ell$ represents the monetary loss caused by a security breach. The parameter $\ell \in \mathbb{R}_+$ is a positive real number. The parameter $v$ represents the probability that without additional security, a threat results in the information set being breached and the loss $\ell$ occurs. The parameter $v$ i called the *vulnerability* of the asset. Being a probability, it belongs to the interval $[0, 1]$.

An agent can invest a certain amount $x$ to reduce the probability of loss to $p(x, v)$. We make the assumptions $p(0, v) = v$ and since $p(x, v)$ is a probability we assume that for all $x > 0$ and $v \in [0, 1]$ we have $0 \leq p(x, v) \leq v$. The function $p(x, v)$ is called the *security breach probability*.

The expected loss for an amount $x$ spent on security is given by $\ell p(x, v)$. Hence if the agent is risk neutral, the optimal security investment should be the value $x^*$ minimizing

$$\min \{\ell p(x, v) + x : x \geq 0\}. \tag{1}$$

We define the set of optimal security investment by

$$\varphi(v, \ell) = \arg\min \{\ell p(x, v) + x : x \geq 0\}$$

Clearly in general the function $\varphi$ is set-valued and we will deal with this fact in the sequel. For now on, assume that the function $\varphi$ is real-valued, i.e. sets reduce to singleton. As noticed in [4], it turns out that the function $\varphi(v, \ell)$ does not need to be non-decreasing in $(v, \ell)$ for general functions $p(x, v)$. In particular, the optimal investment can be zero for low values of the vulnerability and also for high values of the vulnerability. In this case, the marginal benefit from investment in security for low vulnerability information sets does not justify the investment since the security of the information set is already good. However if the information set is extremely vulnerable, the cost of security is too high to be 'profitable', in the sense that there is no benefit in protecting it.

### B. Sufficient conditions for monotone investment

In this section, we derive sufficient conditions on the probability loss in order to avoid the non-monotonicity in the vulnerability of the information set.

First we need to define the monotonicity of a set-valued function. We say that the set-valued function $f : \mathbb{R}^n \to 2^{\mathbb{R}}$ is non-decreasing if for any $x^L, x^H \in \mathbb{R}^n$ with $x^L \leq x^H$ (for the product order), we have for any $y^L \in f(x^L)$ and any $y^H \in f(x^H)$: $y^L \leq y^H$.

We give a particular case and refer to [10] for a more general result (dealing with cases where choices can be discrete):

**Proposition 1.** *Assume that the function $p(x, v)$ is twice continuously differentiable on $\mathbb{R}_+ \times [0, 1]$. If*

$$\frac{\partial p}{\partial x}(x, v) \leq 0, \quad \textit{and,} \quad \frac{\partial^2 p}{\partial x \partial v}(x, v) \leq 0 \tag{2}$$

*then the function $(v, \ell) \mapsto \varphi(v, \ell)$ is non-decreasing in $(v, \ell)$.*

**Remark 1.** *The first condition requires that the function $p(x, v)$ is non-increasing in $x$, i.e. the probability of a security break is lowered when more investment in security is done.*

[2] Note that in this case the risk-neutral assumption made in this paper should be replaced by a risk-adverse assumption.

### C. A simple model and the $1/e$ rule

Even if previous conditions are not met, what is the amount that should be spent on security? The following generalization of Gordon and Loeb's Proposition 3 gives an upper bound on this amount:

**Theorem 1.** *If the function $x \mapsto p(x, v)$ is non-increasing and log-convex in $x$ then the optimal security investment is bounded by $\ell v/e$.*

Theorem 1 shows that for a broad class of information security breach probability function, the optimal security investment is always less than 37% of the expected loss without protection. We refer to [10] for a proof of this theorem and for a natural scenario under which the log-convex assumption is valid.

## III. Optimal security investment for an interconnected agent

We now extend previous framework in order to model an agent who needs to decide the amount to spend on security if this agent is part of a network. In this section, we give results concerning the incentives of an agent in a network. In the next section, we will consider a security game associated to this model of agent and determine the equilibrium outcomes.

### A. General model for an interconnected agent

In order to capture the effect of the network, we will assume that each agent faces an internal risk and an indirect risk. As explained in the introduction, the indirect risk takes into account the fact that a loss can propagate in the network. The estimation of the internal risk depends only on private information available to the agent. However in order to decide on the amount to invest in security, the agent needs also to evaluate the indirect risk. This evaluation depends crucially on the information on the propagation of the risk in the network available to the decision-maker. We now describe an abstract and general setting for the information of the agent.

We assume that the information concerning the impact of the network on the security of the agent is captured by a parameter $\gamma$ living in a partially ordered set $\Gamma$ (poset, i.e a set on which there is a binary relation that is reflexive, antisymmetric and transitive). Indeed this assumption is not a technical assumption. The interpretation is as follows: $\gamma$ captures the state of the network from the point of view of security and we need to be able to compare secure states from unsecure ones.

Given $\gamma \in \Gamma$, the agent is able to compute the probability of loss for any amount $x \in X$ invested in security which is denoted by $p(x, v, \gamma)$. We still assume that the agent is risk neutral , so that the optimal security investment is given by:

$$\varphi(v, \ell, \gamma) = \arg\min\{\ell p(x, v, \gamma) + x : \ x \in X\}. \qquad (3)$$

Note that in our model we consider that only global statistics about the network are available to all agents. The state of the network $\gamma$ is public. A 'high' value of $\gamma$ corresponds to a secure environment, typically with a high fraction of the population investing in security while a 'low' value of $\gamma$ corresponds to an unsecure environment with few people investing in security. For example, in the epidemic risk model described below, decision regarding investment are binary and the public information consists of the parameters of the epidemic risk model (which are supposed to be fixed) and the fraction $\gamma$ of the population investing in security. Then for any $\gamma \in [0, 1]$, the agent is able to compute $p(x, v, \gamma)$ as explained below. Note that in our model, the vulnerability $v$ of an agent is an intinsic parameter of this agent, in particular it does not depend on the behavior of others or $\gamma$.

### B. Epidemic risks model

In order to gain further insight, we consider in this section the case of economic agents subject to epidemic risks. This model was introduced in [5]. We concentrate here on a simplified version presented in [6]. In this section, we focus on the dependence of $p(x, v, \gamma)$ in $x$ and $\gamma$. For ease of notation, we remove the explicit dependence in the vulnerability $v$.

For simplicity, we assume that each agent has a discrete choice regarding self-protection, so that $X = \{0, 1\}$. If she decides to invest in self-protection, we set $x = 1$ and say that the agent is in state $S$ as secure, otherwise we set $x = 0$ and say that the agent is in state $N$ as non-secure or negligent. Note that if the cost of the security product is not one, we can still use this model by normalizing the loss $\ell$ by the cost of the security investment. In order to take her decision, the agent has to evaluate $p(0, \gamma)$ and $p(1, \gamma)$. To do so, we assume that global statistics on the network and on the epidemic risks are publicly available and that the agent uses a simple epidemic model that we now describe.

Agents are represented by vertices of a graph and face two types of losses: direct and indirect (i.e. due to their neighbors). We assume that an agent in state $S$ cannot experience a direct loss and an agent in state $N$ has a probability $p$ of direct loss. Then any agent experiencing a direct loss 'contaminates' neighbors independently of each others with probability $q$ if the neighbor is in state $S$ and $q^+$ if the neighbor is in state $N$, with $q^+ \geq q$. Since only global statistics are available for the graph, we will consider random families of graphs $G^{(n)}$ with $n$ vertices and given vertex degree with a typical node having degree distribution denoted by the random variable $D$ (see [11]). In all cases, we assume that the family of graphs $G^{(n)}$ is independent of all other processes. All our results are related to the large population limit ($n$ tends to infinity). In particular, we are interested in the fraction of the population in state $S$ (i.e. investing in security) and denoted by $\gamma$.

Using this model the agent is able to compute the functions $p(0, \gamma)$ and $p(1, \gamma)$ thanks to the following result proved in [5] and [12] (using a local mean field):

**Proposition 2.** *Let $\Psi(x) = \mathbb{E}[x^D]$ be the generating function of the degree distribution of the graph. For any $\gamma \in [0, 1]$, there is a unique solution in $[0, 1]$ to the fixed point equation:*

$$y = 1 - \gamma\Psi(1 - qy) - (1 - \gamma)(1 - p)\Psi(1 - q^+y),$$

*denoted by $y(\gamma)$. Then we have,*

$$\begin{aligned} p(1,\gamma) &= 1-\Psi(1-qy(\gamma)), \\ p(0,\gamma) &= 1-(1-p)\Psi(1-q^+y(\gamma)). \end{aligned}$$

If we define $h(\gamma) = p(0,\gamma) - p(1,\gamma)$ as the difference of the two terms given in Proposition 2, we see that the optimal decision is:

$$\ell h(\gamma) > 1 \quad \Leftrightarrow \quad \text{agent invests.} \tag{4}$$

If the benefit of the protection which is $\ell h(\gamma)$ is more than its cost (here normalized to one), the agent decides to invest, otherwise the agents does not invest. In particular, we observe that the condition for the incentive to invest in security to increase with the fraction of population investing in security is given by:

$$h(\gamma) = p(0,\gamma) - p(1,\gamma) \text{ is a decreasing function.} \tag{5}$$

We refer to [10] for a generalization of this property to a much more general framework and the study of two cases with strong and weak protection.

## IV. Equilibrium analysis of the security game

We now present our results in a game-theoretic framework where each agent is strategic. We assume that the effect of the action of any single agent is infinitesimal but each agent anticipates the effect of the actions of all other agents on the security level of the network.

### A. Information structure and fulfilled expectations equilibrium

In most of the literature on security games, it is assumed that the player has complete information. In particular, each player knows the probability of propagation of the attack or failure from each other player in the network and also the cost functions of other players. In this case, the agent is able to compute the Nash equilibria of the games (if no constraint is made on the computing power of the agent) and decides on her level of investment accordingly. In particular, the agent is able to solve (3) for all possible values of $\gamma$ which capture the decision of all other agents. Note that even if only binary decisions are made by agents the size of the set $\Gamma$ grows exponentially with the number of players in the network. Moreover in a large network, the complete information assumption seems quite artificial, especially for security games where complete information would then implies that the agents disclose information on their security strategy to the public and hence to the potential attacker!

Here we relax the assumption of complete information. As in previous section, we assume that each agent is able to compute the function $p(x,v,\gamma)$ based on public information and on the epidemic risk model. The values of the possible loss $\ell$ and the vulnerability $v$ are private information of the agent and vary among the population. In order to define properly the equilibrium of the game, we assume that all players are strategic and are able to do this computation. Hence if a player expect that a fraction $\gamma^e$ of the population invests in security, she can decide for her own investment. We assume that at equilibrium expectations are fulfilled so that at equilibrium the actual value of $\gamma$ coincides with $\gamma^e$. This concept of fulfilled expectations equilibrium to model network externalities is standard in economics (see Section 3.6.2 in [2]).

We now describe it in more details. For simplicity of the presentation, we do not consider the dependence in the vulnerability $v$ since in the security game, we focus on the monotonicity in $\gamma$ which will turn out to be crucial. We also consider that the choice regarding investment is binary, i.e. $X = \{0,1\}$.

We consider a heterogeneous population, where agents differ in loss sizes only. This loss size $\ell$ is called the type of the agent. We assume that agents expect a fraction $\gamma^e$ of agents in state $S$, i.e. to make their choice, they assume that the fraction of agents investing in security is $\gamma^e$. We now define a network externalities function that captures the influence of the expected fraction of agents in state $S$ on the willingness to pay for security. Let the network externalities function be $h(\gamma^e)$. More precisely, for an agent of type $\ell$, the willingness to pay for protection in a network with a fraction $\gamma^e$ of the agents in state $S$ is given by $\ell h(\gamma^e)$ so that if

$$\ell h(\gamma^e) \geq c, \text{ (where } c \text{ is the cost of the security option)} \tag{6}$$

the agent will invest and otherwise not. Hence (6) is in accordance with (4) (where the cost was normalized to one). Note that here, we do not make any a priori assumption on the network externalities function $h$ which can be general and fit to various models.

Let the cumulative distribution function of types be $F(\ell)$, i.e the fraction of the population having type lower than $\ell$ is given by $F(\ell) \leq 1$. We assume that $F(\ell)$ is continuous with positive density everywhere on its support which is normalized to be $[0,1]$. In particular, $F$ is strictly increasing and it follows that the inverse $F^{-1}(\gamma)$ is well-defined for $\gamma \in [0,1]$.

Given expectation $\gamma^e$ and cost for protection $c$, all agents with type $\ell$ such that $\ell h(\gamma^e) > c$ will invest in protection. Hence the actual fraction of agents investing in protection is given by $\gamma = 1 - F\left(\min\left(\frac{c}{h(\gamma^e)}, 1\right)\right)$. Hence, we can invert this equation and we define the willingness to pay for the last agent in a network of size $\gamma$ with expectation $\gamma^e$ as

$$w(\gamma,\gamma^e) = h(\gamma^e)F^{-1}(1-\gamma). \tag{7}$$

Seen as a function of its first argument, this is just an inverse demand function: it maps the quantity of protection demanded to the market price. For goods that do not exhibit network externalities, demand slopes downward: as price increases, less of the good is demanded. This fundamental relationship may fail in goods with network externalities.

For a fixed cost $c$, in equilibrium, the expected fraction $\gamma^e$ and the actual one $\gamma$ must satisfy

$$c = w(\gamma,\gamma^e) = h(\gamma^e)F^{-1}(1-\gamma). \tag{8}$$

If we assume moreover that in equilibrium, expectations are fulfilled, then the possible equilibria are given by the fixed point equation:

$$c = w(\gamma,\gamma) = h(\gamma)F^{-1}(1-\gamma) =: w(\gamma). \tag{9}$$

We see that if $h'(.) > 0$, the concept of fulfilled expectations equilibrium captures the possible increase in the willingness to pay as the number expected to be sold increases. This would corresponds to the case where we have $w'(\gamma) > 0$ for some values of $\gamma$. In such cases, a critical mass phenomenon can occurs: there is a problem of coordination. We explain this phenomenon more formally in [10].

**Remark 2.** *The case of an homogeneous population in which all agents have the same type, i.e the same loss size $\ell$ corresponds to the function $F^{-1}$ being constant equal to $\ell$. In this case, the willingness to pay is simply $w(\gamma) = h(\gamma)\ell$. In particular, the epidemic risk model presented above can be used to model the network externalities by the function $h(\gamma)$ computed in Section III. In this case, Condition (5) still gives a condition for incentives to be align. As shown in [10], this condition prevents critical mass: there is no coordination problem.*

### B. Critical mass: coordination problem

To determine the possible equilibria, we analize the shape of the fulfilled expectations demand $w(\gamma)$. We refer to [10] for this analysis and the proof of the following theorem:

**Theorem 2.** *A network has positive critical mass if $\lim_{\gamma\to 0} h'(\gamma) > 0$ and either*

(i) $w(0) = 0$*, i.e. if all agents are in state $N$ then no agent is willing to invest in self-protection;*

(ii) $\lim_{\gamma\to 0} h'(\gamma)$ *is sufficiently large, i.e. there are large private benefits to join the group of agents in state $S$ when the size of this group is small;*

(iii) $\lim_{\gamma\to 1} F'(\gamma)$ *is sufficiently large, i.e. there is a significant density of agents who are ready to invest in self-protection even if the number of agents already in state $S$ is small.*

We finish this section by explaining the main difference between our model and models with standard positive externalities which are felt only by the adopters of the good. In our case, when an agent chooses to invest in security, we have to distinguish between two positive externalities: one is felt by the agents in state $S$ and the other is felt by the agent in state $N$. Indeed as $\gamma$ increases, both populations expereince a decrease of their probability of loss but the value of this decrease is not the same in both populations. We call the 'public externalities' the decrease felt by agents in state $N$ and the 'private externalities' the decrease felt only by agents in state $S$. We can still have $h'(.) < 0$ so that by result of previous section (see Condition 5), incentives are align and there is no coordination problem (no critical mass). However, we show in [10] that even in this case, the equilibrium is not socially efficient:

**Theorem 3.** *A social planner will choose a larger fraction $\gamma$ of agents investing in self-protection than the market equilibrium for any fixed cost $c$.*

## V. Conclusion

In this paper, we study under which conditions agents in a large network invest in self-protection. We started our analysis with finding conditions when the amount of investment inceases for a single agent as the vulnerability and loss increase. We also showed that risk-neutral agent do not invest more than 37% of the expected loss under log-convex security breach probability functions. We then extended our analysis to the case of interconnected agents of a large network using a simple epidemic risk models. We derived a sufficient condition on the security breach probability functions taking into consideration the global knowledge on the security of the entire network for guaranteeing increasing investment with increasing vulnerability. It would be interesting to use other epidemics models as in [13] to see the impact on the results of this section. Finally, we study a security game where agents anticipate the effect of their actions on the security level of the network. We showed that the condition derived to ensure the monotinicity of investment of an interconnected agent with respect to the global security level of the netwok, also ensures that there is no coordination problem. In the case of an homogeneous population, we showed that even if the incentives are aligned, the fulfilled equilibrium is not socially efficient. We explained it by the separation of the network externalities in two components: one public (felt by agents not investing) and the other private (felt only by agents investing in self-protection).

## References

[1] R. Anderson, "Why information security is hard-an economic perspective," in *ACSAC '01: Proceedings of the 17th Annual Computer Security Applications Conference*. Washington, DC, USA: IEEE Computer Society, 2001, p. 358.

[2] J. Farrell and P. Klemperer, *Coordination and Lock-In: Competition with Switching Costs and Network Effects*, ser. Handbook of Industrial Organization. Elsevier, 2007, vol. 3, ch. 31, pp. 1967–2072.

[3] H. R. Varian, "System reliability and free riding," in *in Economics of Information Security, Kluwer 2004 pp 115*. Kluwer Academic Publishers, 2002, pp. 1–15.

[4] L. Gordon and M. Loeb, "The economics of information security investment," *ACM transactions on information and system security*, vol. 5, no. 4, pp. 438–457, 2002.

[5] M. Lelarge and J. Bolot, "Network externalities and the deployment of security features and protocols in the internet," in *SIGMETRICS '08*. New York, NY, USA: ACM, 2008, pp. 37–48.

[6] M. Lelarge, "Economics of malware: Epidemic risks model, network externalities and incentives," in *Allerton*, 2009.

[7] J. Bolot and M. Lelarge, "A New Perspective on Internet Security using Insurance," in *IEEE INFOCOM*, 2008, pp. 1948–1956.

[8] ——, "Cyber Insurance as an Incentive for Internet Security," in *Workshop in Economics of Information Security (WEIS) Seventh Workshop on Economics of Invormation Security, June*, 2008, pp. 25–28.

[9] M. Lelarge and J. Bolot, "Economic Incentives to Increase Security in the Internet: The Case for Insurance," in *IEEE INFOCOM*, 2009.

[10] M. Lelarge, "Coordination in network security games: a monotone comparative statics approach," Tech. Rep., 2012.

[11] R. Durrett, *Random graph dynamics*, ser. Cambridge Series in Statistical and Probabilistic Mathematics. Cambridge: Cambridge University Press, 2007.

[12] M. Lelarge and J. Bolot, "A local mean field analysis of security investments in networks," in *NetEcon '08*. New York, NY, USA: ACM, 2008, pp. 25–30.

[13] M. Lelarge, "Diffusion and cascading behavior in random networks," Tech. Rep., 2011.