# Network Effects in the Security Software Market*

**Debabrata Dey** (ddey@uw.edu)
**Atanu Lahiri** (lahiria@uw.edu)

University of Washington, Michael G. Foster School of Business, Seattle, WA 98195, USA

**Guoying Zhang** (grace.zhang@mwsu.edu)

Midwestern State University, Dillard College of Business, Wichita Falls, TX 76308, USA

August 29, 2011

**Abstract**

The market for security software has witnessed an unprecedented growth in recent years. A closer examination of this market reveals certain idiosyncrasies that are not observed in a traditional software market. For example, it is a highly competitive market involving many vendors. Yet, the market coverage seems relatively low. Prior research has not attempted to explain what makes this market different. In this paper, we develop a quantitative model to find possible answers to this question. Our model identifies a possible reason behind this behavior—that of a negative network effect, a phenomenon that has received considerable attention in the recent literature on application software security. Overall, our results highlight the unique nature of the security software market, furnish rigorous explanations for several counter-intuitive observations in the real world, and provide managerial insights for vendors on market competition.

**Keywords**: Security software, network effect, oligopoly, market structure, pricing.

## 1 Introduction

In a society that depends on computer-based systems and networks for almost everything, security of computerized systems is equally critical for both individuals and organizations. Because of the severe need for protecting valuable information assets in today's networked world, the industry of security software, along with those of hardware and services, has grown rapidly. Figure 1, which is based on data provided by Gartner Group, shows how rapidly the worldwide *security software* market has expanded in recent years. As can be seen from the figure, it has grown substantially from US$6.4 billion in 2004 to about US$16.6 billion in 2010; even a worldwide recession in 2009 did not slow this market down. This rapid growth has exceeded expectations. Gartner Group earlier predicted that the worldwide market would be about US$13.5 billion in 2011 (Latimer-Livingston and Contu 2007), but that level was reached as early as 2008. IDC has reported that the security

*We would like to thank the participants of the weekly seminar series at the Department of Marketing and International Business and the Department of Information Systems and Operations Managment, Michael G. Foster School of Business, University of Washington, Seattle, WA; this paper has benefited from their constructive comments. Draft Only; please do not quote or circulate without permission.

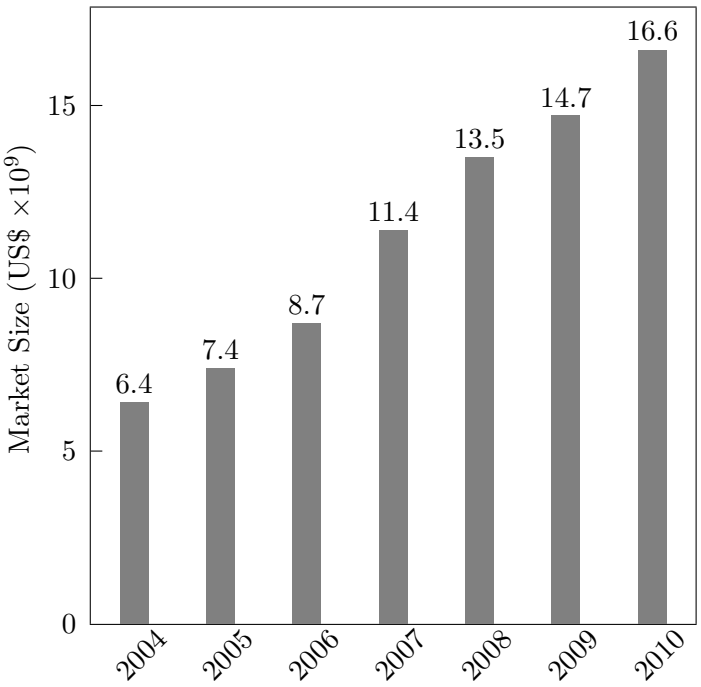



Figure 1: Growth of Worldwide Security Software Market

software market in Asia (excluding Japan) alone demonstrated about 23% growth in 2005, and it has since been keeping pace with the rest of the world (Low and Chung 2006). Security software market, because of its double-digit growth rate, has indeed become one of the prominent software markets (McCormack 2006). Understanding the nature of this market, along with its evolution and trend, is of importance to vendors as well as consumers.

In general, security software can be classified into two main categories: (i) third-party standalone tools, such as antivirus software and spyware remover, and (ii) system components, such as encryption software and firewall that are often bundled with the operating system. The security software market is overwhelmingly dominated by the first category. This category has several major players including Symantec, Trend Micro, McAfee, Computer Associates, and dozens of other smaller companies.[1] Therefore, in this paper, we examine the first category.

In the typical off-the-shelf software market, users usually enjoy a higher network utility derived from a larger market share, which is often referred to as the positive network effect (Katz and

[1]Just to name a few, consider products such as Kaspersky, Avast, Sophos, AVG, Bitdefender, Panda, Avira, G-Data, F-Secure, Webroot, ESET, Lavasoft, Vipre, PCTools, SystemShield, SpySweeper, SuperAntiSpyware, SystemTech, SystemWorks, Virex, Iolo, Forefront, Avira, G-DATA, Kaseya, Ad-Aware, Outpost, Digital Defender, Immunet Protect, Zone Alarm, Websense, and VCatch.

Shapiro 1985, 1986). This positive network effect primarily arises from users' need for compatibility—the need to share files and information, to edit and critique documents created by others, and, most importantly, to work in a collaborative setting. It is well-known that positive network effect can lead to a near-monopoly market condition: if a vendor's market share is large enough to exceed a critical mass, other competitors will lose opportunities to enter the market (Shapiro and Varian 1999). Studies on markets for off-the-shelf application software, such as spreadsheets and word processors, empirically validate this near-monopolistic structure (Brynjolfsson and Kemerer 1996, Liebowitz and Margolis 1999).

The market for third-party security software, however, is markedly different. As mentioned above, this market is characterized by many vendors, with no single dominant player. Symantec, which once led this market with more than 50% of the industry sales, currently holds less than 20% of the market share. In fact, the total market share of the top 6 antivirus software vendors is well below 50%. Many of the current antivirus products in the market did not exist even a couple of years ago. Fosfuri and Giarratana (2004) found that, between 1989 and 1998, at least 270 vendors entered this market, with a very high percentage not surviving beyond the first two years (Giarratana 2004). Despite a large number of vendors, the price for this type of software has remained relatively high. For example, an annual subscription of *Kaspersky Internet Security 2012* software can cost as much as $80. At the same time, a two-year subscription can cost up to $120, comparable to the cost of Microsoft Word 2010, a product that enjoys substantial monopoly power. Furthermore, in spite of this large number of vendors, a significant percentage of individual computers are still lacking in basic protection (Gordon and Loeb 2002, Lacy 2006). A recent study on online banking finds that as many as 47% of household finance managers (i.e., those who manage their household finances using online banking) do not use any antivirus software (Eichorn and Smith 2011). These observations naturally lead to several questions:

- Why is the market coverage so low despite the market being competitive?
- What explains such high prices in a competitive market?
- What makes this market so attractive to new entrants?

The objective of this research is to develop a quantitative model to find possible answers to these questions and obtain useful insights about the market.

It is difficult to explain the competitiveness observed in this market under the assumption of positive network effect. In reality, positive network effect is unlikely to be significant for most security software. Security software is simply used to prevent security exploitations, and there is hardly any benefit from the compatibility of user data. Consequently, the market for security software does not exhibit as strong a positive network effect as many other software markets do.[2]

We, therefore, start with a setting that has no positive network effects. In our setting, when a user adopts a security software, there are two benefits: (i) a direct benefit—representing the value of thwarting direct security attacks by hackers, and (ii) an indirect benefit—arising from the prevention of indirect attacks or infection from other users in the network (Ogut et al. 2005). In the case of an indirect attack, a system is not a direct target, but could become an eventual target from the security exploitation of another system. Examples of indirect attacks abound, as evidenced by the prevalence of internet worms (Braverman 2005) and the wide presence of botnet agents that can launch large-scale attacks with the ability to convert ordinary nodes into malicious agents (Goodchild 2011, Sancho 2005). A recent report finds that most of the well-known botnets involve several million bots or compromised computers—for example, the *Bredolab* and *Conflicker* botnets are supposed to have about 30 and 13 million infected machines, respectively (Goodchild 2011). Each month, hundreds of thousands of new machines are being added to some botnet. The total annual loss from this type of indirect attacks is currently estimated at a whopping US$10 billion (Goodchild 2011).

In our model, the user's indirect benefit eventually leads to a type of negative network effect, similar to that in (August and Tunca 2006, 2008, 2011). The larger the total market coverage of security software, the less is the indirect benefit because the chance of getting infected from others reduces. Such indirect effects have also been recognized by Anderson (2001) as the "tragedy of commons," and by Png et al. (2006) as the "the reason of users' inertia of taking security precautions."

[2]We should point out that, while compatibility concern is the primary force behind the positive network effect in off-the-shelf software markets (Gandal 1995), there may well be other contributing factors for this effect. For example, a larger market share of a product may provide additional utility to a user in terms of better product support, availability of helpful tips and resources (such as end-user forums), and better maintenance (in terms of more frequent updates and upgrades). Since these are all applicable to a security software, there may indeed be some positive network effect in this market as well. However, since the major factor (compatibility) is missing in this context, the positive network effect is significantly weaker here, when compared to the typical software market.

We examine different market situations. We start by analyzing a monopoly market with negative network effect. We show that the monopolist reduces her market coverage and charges a higher price when the network effect increases. By reducing coverage, the monopolist is able to charge substantially for indirect benefits, which translates to a higher revenue vis-à-vis a traditional monopoly market (i.e., one without network effects).[3]

We then extend our analysis to oligopoly competition. There is a unique symmetric equilibrium in the oligopoly market: as negative network effect increases, the equilibrium price rises but the market coverage contracts, in a manner similar to what happens in the monopoly market. Therefore, even in a competitive setting, the presence of modest levels of negative network effect seems to explain several characteristics of the security software market, such as the prevalence of higher prices and lower coverage, which otherwise appear counterintuitive.

We further find that, notwithstanding the shrinking market coverage, the industry makes higher profits by charging consumers handsomely for indirect benefits that are often substantial in a deficiently covered market. This higher profitability means that an oligopoly market with negative network effect is going to have more competitors in the long-run when compared to a market without such an effect. Perhaps, as the world has become more connected, and indirect threats have risen, negative network effect has made it possible for the industry to increases prices and profits while dropping coverage. At the same time, higher prices and inadequate coverage have attracted new entrants and made the market more competitive over the long run. We carefully study the effect of a new entry into the oligopoly market and find that the new entrant is likely to adopt a more aggressive market strategy here than in a traditional market. Thus, we again find that, when negative network effect is included in the economic analysis, it furnishes results that coincide with the unique nature of the security software market.

The rest of the paper proceeds as follows. In Section 2, we review the related literature. We develop consumer models for monopoly and oligopoly settings in Section 3. In Section 4, we evaluate the market structure under the influence of negative network effect; we also discuss how this influence may explain the realities of the security software market. In Section 5, we present two extensions to our basic model and prove the applicability of our results in wider settings. Section 6 provides a summary of our work and offers directions for future research.

[3]Following Katz and Shapiro (1985), throughout this paper, we use the traditional market, i.e., a market without any network effect, as the benchmark for understanding the impact of network effect.

## 2 Literature Review

The behavior of a market for a technology product in the presence of positive network effect has been extensively studied (Basu et al. 2003, Economides 1996, Farrell and Saloner 1986, Katz and Shapiro 1985, 1986). This stream of research recognizes the existence of an additional utility, which depends on the vendor's market size, in addition to the utility derived directly from the product. Most subsequent studies on software markets have made this positive network externality, and the resulting monopoly structure, a common assumption. Although there is a long stream of research on positive network effects in software markets, there exists limited research on negative network effects and how they may impact the structure and competition in these markets.[4] Our aim is to fill this void.

The market for security software is unique because a user's valuation diminishes with an increasing market size (Ogut et al. 2005). Png et al. (2006) identify negative network effect to be a possible explanation for users' inertia in taking security precautions. August and Tunca (2006, 2008) also recognize the existence of negative network effect and develop an economic model in which a consumer's valuation for an application software—or an operating system—depends on the number of unpatched vulnerable copies of that software in the user network. According to them, the larger the number of vulnerable nodes, the greater is the chance of an indirect infection. One of their major conclusions is that, when this effect is sufficiently large, the vendor has an incentive to support pirates with security patches in order to effectively mitigate its influence.

The form of negative network effect discussed in this paper is not new, and it has been amply discussed by August and Tunca (2006, 2008). However, there is a fundamental difference between their work and ours. In their case, the subject of the study is an application software vendor: a large negative network effect reduces the value consumers get from the product and reduces her pricing power. In our case, the context is the security software market, which is essentially a mirror image of the application software market: a large negative network effect here threatens consumers even more, increasing their willingness-to-pay (WTP) for security solutions. Also, driven by the realities of the third-party security software market, we devote a considerable part of our work on competitive settings, whereas August and Tunca (2006, 2008) primarily dwell on the monopoly

[4] Although there is extensive literature on negative externalities that arise out of congestions in service systems (e.g., Zhang et al. (2007)), work on negative network effect in software markets is quite limited.

scenario. Another difference is that we examine different types of security-related network effects (in Section 5) and, in doing so, relax their assumption that network effect is always proportional to the number of vulnerable machines.

The negative network effect studied in this research is also related to the literature on the "snob effect," a term used to refer to the reduction in individual demand with increasing aggregate demand (Leibenstein 1950); it represents the social desire of consumers to be different from others (such as, in the consumption of expensive cars and jewelry). In the presence of this effect, the aggregate demand curve becomes relatively more inelastic. Grillo et al. (2001) combine this externality with spatial duopoly models and show that this "vanity" leads to a higher price equilibrium, because it translates to a less elastic demand for each firm, diminishing the incentive to reduce prices. However, in their paper, network externalities are associated with an exogenous population size, whereas, in our study, the network effect is based on a market size that is endogenous and is obtained from a "fulfilled expectations equilibrium" (Katz and Shapiro 1985). Finally, the snob effect has its root in the personal perception of an individual to dissociate from others, whereas the negative network effect in the security software market is derived from the value obtained from thwarting indirect infections.

Our research is at the intersection of network effects and information systems security. The stream on security has also grown substantially in recent years. Gordon and Loeb (2002) consider the investment decision for information system security and develop an economic model that trades off the cost of security with the expected loss from attacks. In a subsequent empirical work, Gordon and Loeb (2006) find that this kind of economic analysis is widely used in practice for security investment decisions. Chen et al. (2005) examine the issue of investing in heterogeneous IT infrastructure by considering a diversified portfolio of platforms. They consider both positive (accruing from compatibility and interoperability) and negative (ensuing from security attacks geared towards a more popular platform) network externalities and find that diversification not only reduces the variance of security loss but also minimizes the expected loss. Further evidence of the benefit of diversification is provided by Böhme (2005), who finds that system diversity is preferred by an insurance issuer. Just as hackers target popular systems, in some cases, they target vulnerable computers. This is because hackers are utility-maximizing agents (Ransbotham and Mitra 2009) and they often choose targets in a way that their chances of succeeding are maximized.

Interestingly, as we explain in Section 5, targeting of insecure nodes leads to a positive network effect in the security software market. We explain its implications for the market and vendors.

Ogut et al. (2005) recognize that IT security risks borne by organizations in a networked environment are interdependent and show that this interdependence reduces an organization's incentives to invest in security technologies or to buy cyber-insurance coverage. Gal-Or and Ghose (2003) and Gordon et al. (2003) study the economic and social effects of sharing the information on security breaches among organizations. Kannan and Telang (2005) study whether a market mechanism can replace the social planner; they consider an infomediary who provides monetary rewards to vulnerability identifiers and charges his customers a subscription fee for sharing the vulnerability information. They find that, from an overall social welfare perspective, a social planner outperforms the market mechanism. Anderson (2001), Anderson and Moore (2006), and Varian (2000) look at the provision of security from the perspectives of underlying incentives, legal liability, and network externalities. Ghose and Sundararajan (2005) analyze bundling of different security software components. They analytically show that a mixed bundling strategy is superior to pure bundling and find preliminary empirical evidence to that effect, as well. Giarratana (2004) undertakes an empirical analysis of the number of existing vendors in the security software industry. Fosfuri and Giarratana (2004) evaluate the post-entry strategy for startups in this industry. These last two studies are of particular interest to us, as they reveal the extreme level of fragmentation existing in the market for security software. The question that we answer here is: to what extent does the presence of negative network effect explain this market structure? We also examine whether it explains other counterintuitive observations, such as the pervasiveness of high prices and low coverage in spite of the presence of a large number of competing firms.

## 3 The Model

Consumers (users) of security software are heterogeneous because the amount of benefit from thwarting an attack would vary from user to user. In order to capture this, consumers are indexed by a parameter $u$ that indicates their relative expected benefit if an attack is thwarted; we assume that $u$ is uniformly distributed over the interval $[0, 1]$. The absolute expected benefit to user $u$ from thwarting an attack can then be expressed as $Lu$, where $L$ is a constant; $Lu$ can also

be viewed as a proxy for the potential loss to user $u$ from an attack (Gordon and Loeb 2002).

As mentioned in Section 1, there are two types of benefits derived from adopting a security software—direct and indirect. First, consider the direct benefit. Assume that hackers could launch successful attacks on an unprotected system at an average rate of $\lambda_D$. Therefore, by adopting a security software, user $u$ has a direct mitigation benefit rate of $\lambda_D Lu$.

Next, we consider the indirect benefit. Given the current level of internet adoption and the increasingly popular broadband technology, users' computers are considered to be interconnected. Therefore, unprotected systems might replicate malicious codes and pass them to connected peers. At times, a hacker may attack a system indirectly, after first breaching the security of several other systems and using them as intermediate nodes to launch the attack. In other words, the existence of security software in one system can, indirectly, reduce attacks to others. Let $x$ be the fraction of users who have adopted security software. Then, an indirect attack is possible from the $(1-x)$ unprotected fraction of users, so we model the rate of indirect attack as $\lambda_I(1-x)$, where $\lambda_I$ is the base rate of indirect attack (when no user is protected).[5] Therefore, a user adopting a security software avoids indirect attacks from the unprotected users and derives an indirect utility of $\lambda_I(1-x)Lu$. It is now obvious that a larger market share (larger $x$) leads to a reduction in this indirect utility. At the extreme, if all the users are equipped with security software, *no* user derives any indirect benefit. This is similar to the free riding behavior in network systems and the feature of public goods in economics (Anderson 2001, Png et al. 2006).

The total benefit (per unit time) to user $u$ from adopting the software, in a market with coverage $x$, can then be written as:

$$B_u = \lambda_D Lu + \lambda_I(1-x)Lu = \lambda_D Lu\left(1 + g(1-x)\right), \tag{1}$$

where $g = \frac{\lambda_I}{\lambda_D}$. Clearly, the parameter $g$ is a proxy for the negative network effect—the higher is $g$, the larger is the potential indirect benefit and the more significant is the negative network effect. Writing the above expression in this form provides us with the flexibility to easily capture various levels of the relative indirect utility, which can be attributed to factors such as the network connectivity—a well-connected network is likely to have a higher value of $g$, when compared to a

[5]The assumption that the rate of indirect attacks is proportional to the fraction of vulnerable nodes in the network is quite similar to the assumptions made by August and Tunca (2006, 2008, 2011).

sparser network.

Two points are worth mentioning here. First, not all attacks result in security breaches. At the same time, a security software may not be fully effective in thwarting an attack. These considerations may lead one to suspect that the benefit of a security software to a user is overestimated by $B_u$ in Equation (1). However, this issue does not impact our modeling choice because both $\lambda_D$ and $\lambda_I$ can be suitably scaled to reflect this situation. As a second related point, individual users or organizations may deploy complementary technologies that may have an impact on a user's benefit from a security software. For example, if firewalls or intrusion prevention systems are widely used, they may reduce the effective attack rates and, therefore, reduce the overall valuation of an antivirus software. Again, this issue can be addressed by similar scaling as above.

Security software products are usually licensed as a subscription for a year. Upon expiration, the user must renew the license to continue getting the service. Let $P$ be the subscription price (per unit time). A user would adopt a security software if the total benefit from the software is larger than its subscription price: $B_u \geq P$. The marginal user $u$ who is indifferent between adopting and not adopting the security software must then satisfy the following condition:[6]

$$\lambda_D L u \left(1 + g(1-x)\right) - P = 0.$$

As shown in Figure 2, any user to the right of this marginal user adopts the software, whereas anyone to the left does not. Therefore, $u = 1 - x$. Substituting this and letting $p = \frac{P}{\lambda_D L}$, we get:

$$p = \left(1 + g(1-x)\right)(1-x). \tag{2}$$

Equation (2) represents the normalized price associated with a market coverage of $x$. For the rest of the paper, we will use this normalized price, with appropriate subscripts, as necessary. Interested reader may recognize the correspondence of Equation (2) with its counterpart for a market with positive network effect. In the case of positive network effect, the WTP of the marginal user could be written as:

$$p = (1 + \gamma x)(1 - x),$$

[6]We should point out that, in this analysis, we are using the concept of fulfilled expected equilibrium (Katz and Shapiro 1985)—the user makes the adoption decision based on an expected value of the market size, and the realized markets size in equilibrium equals this expected value.

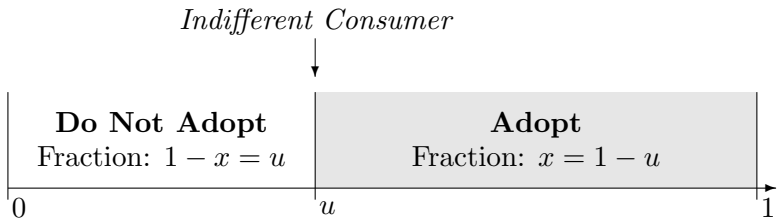



Figure 2: Consumers Choose to Adopt (or Not Adopt) Based on Their Relative Benefit

where $\gamma$ is a parameter representing the strength of positive network effect. In both cases, network effect increases the willingness-to-pay (WTP); however, the WTP decreases with $x$ in our model, whereas it increases in the case of positive network effect.

### 3.1 Monopoly Market

Existing literature on the economics of software and information goods often view a software market as a natural monopoly. We, therefore, start our analysis with the monopoly market. Let the monopoly market coverage be $x_{\text{mon}}$; from Equation (2), the corresponding normalized price is given by:

$$p_{\text{mon}} = (1 + g(1 - x_{\text{mon}}))(1 - x_{\text{mon}}). \tag{3}$$

Therefore, with a zero marginal cost for each user's subscription, the monopolist's objective is to select the optimal market coverage to maximize her revenue. More specifically, the monopolist solves the following optimization problem:

$$\underset{x_{\text{mon}}}{\text{Max}}\, R_{\text{mon}} = p_{\text{mon}} x_{\text{mon}};\ 0 \leq x_{\text{mon}} \leq 1. \tag{4}$$

Solving (4), we get the following result:

**Proposition 1.** *In the monopoly market described above, the optimal market share and price are:*

$$x^*_{\text{mon}} = \frac{(2g+1) - \sqrt{g^2+g+1}}{3g},\ \textit{and} \tag{5}$$

$$p^*_{\text{mon}} = \frac{(2g^2+2g-1)+(2g+1)\sqrt{g^2+g+1}}{9g}. \tag{6}$$

It can be shown that the results in Proposition 1 converge to those in a traditional monopoly

market; in other words:

$$\lim_{g\to 0} x^*_{\text{mon}} = \frac{1}{2},\ \lim_{g\to 0} p^*_{\text{mon}} = \frac{1}{2},\ \text{and}\ \lim_{g\to 0} R_{\text{mon}}(x^*_{\text{mon}}) = \frac{1}{4}.$$

**Corollary 1.** *The monopoly market described above has a smaller market coverage, higher price, and higher revenue, when compared to a monopoly market without network effects.*

The result above simply means that, if negative network effect is not accounted for, it would be difficult to explain the prevalence of higher prices and lower coverage commonly observed in the security software market. It thus appears that a meaningful analysis of the security software market would require taking into consideration the existence of this network effect.

In any case, the monopoly setting is not quite relevant to the context of security software. We, therefore, examine the impact of incorporating this network effect into an analysis of an oligopoly.

### 3.2 Oligopoly Market

We apply the concept of fulfilled expected Cournot equilibrium (Katz and Shapiro 1985) to study the oligopoly competition. We use the Cournot competition to model the relatively long-term decisions by vendors and use the market size as the decision variable for vendors. Cournot competition fits this context a lot better than Bertrand competition. A large majority of subscriptions to security software happens through preloading contracts with computer manufacturers. All leading security software vendors engage in such long-term contractual agreements with them. Some of these contracts are exclusive, while others are not. For example, Dell has a *non-exclusive* contract with Symantec, McAfee, and Trend Micro to preload their antivirus software on all the computers they sell to consumers. On the other hand, HP currently has an *exclusive* contract with Symantec. Consumers get a free trial period for the preloaded software, but must purchase the subscription if they wish to continue using it beyond the trial period. Engaging in this kind of long-term preloading contracts means that a vendor plans how many subscriptions it intends to sell, since the price she is willing to pay for the preloading contract is contingent on the expected sales. As shown by Kreps and Scheinkman (1983), when vendors plan for a certain quantity in the first stage, a Bertrand-like price competition would still lead to a Cournot equilibrium, even if the marginal production cost is zero.

It is also instructive to see why the alternative, Bertrand competition, does not work in this setting. First, a pure Bertrand would drive the price down to zero—not something that is observed in practice. Second, a differentiated Bertrand—the circular city (Salop 1979) or the linear city (Hotelling 1929) model—would require a complete coverage of the market for real competition to set in. As mentioned earlier, assuming complete coverage would be contrary to real-world observations.

Suppose that, in equilibrium, there are $n$ identical vendors in the market with non-negative revenue. The aggregate market size is $M$, where $M = \sum_{i=1}^{n} x_i$, and $x_i$ is vendor $i$'s market size. We define $\sum x_{-i}$ as the total market size of all vendors except that of vendor $i$, i.e., $\sum x_{-i} = M - x_i$. Extending Equation (2) for a total market coverage of $M$, we find that the price in this case would be $(1 + g(1 - M))(1 - M)$, which is the valuation of the marginal user indifferent between adopting and not adopting security software. For vendor $i$, the revenue maximization problem can, therefore, be formulated as:

$$\underset{x_i}{\text{Max}}\, R_{\text{olig}} = \left(1 + g\left(1 - \sum x_{-i} - x_i\right)\right)\left(1 - \sum x_{-i} - x_i\right) x_i; \;\; 0 \leq \sum_{i=1}^{n} x_i \leq 1. \tag{7}$$

We can solve (7) to obtain the following result:

**Proposition 2.** *In the oligopoly market with n identical vendors, the equilibrium market size and price for each vendor are given by:*

$$x^*_{\text{olig}} = \frac{(2g+1)(1+n) - \sqrt{4g(g+1) + (1+n)^2}}{2gn(2+n)}, \text{ and} \tag{8}$$

$$p^*_{\text{olig}} = \frac{4g(g+1) - (1+n) + (2g+1)\sqrt{4g(g+1) + (1+n)^2}}{2g(2+n)^2}. \tag{9}$$

It can be shown through algebraic manipulations that the results in Proposition 2 converge to those in a traditional oligopoly market:

$$\lim_{g \to 0} x^*_{\text{olig}} = \frac{1}{n+1}, \;\; \lim_{g \to 0} p^*_{\text{olig}} = \frac{1}{n+1}, \;\; \text{and} \;\; \lim_{g \to 0} R_{\text{olig}}(x^*_{\text{olig}}) = \frac{1}{(n+1)^2}.$$

Before proceeding with a discussion of the market structure, the following result is necessary:

**Corollary 2.** *The oligopoly market has the following characteristics:*

$$\frac{\partial x^*_{\text{olig}}}{\partial g} \leq 0,\ \frac{\partial x^*_{\text{olig}}}{\partial n} \leq 0,\ \frac{\partial p^*_{\text{olig}}}{\partial g} \geq 0,\ \frac{\partial p^*_{\text{olig}}}{\partial n} \leq 0,\ \frac{\partial R_{\text{olig}}\left(x^*_{\text{olig}}\right)}{\partial g} \geq 0,\ \textit{and}\ \frac{\partial R_{\text{olig}}\left(x^*_{\text{olig}}\right)}{\partial n} \leq 0.$$

# 4 Market Structure

In this section, we use the results from the model to analyze the structure of a market with negative network effect and examine if it is consistent with that of the security software market.

## 4.1 Equilibrium Coverage and Price

We have already discussed that the security software market has higher price and lower coverage, an observation that is consistent with the oligopoly model described above:

**Theorem 1.** *The oligopoly market described above has a smaller market coverage and higher price, when compared to an oligopoly market without network effects.*

Theorem 1 shows that incorporating negative network effect into the economic analysis leads to realistic results in the oligopoly setting as well. Without considering this network effect, it is not plausible to explain many real-world observations, e.g., many antivirus products commanding a price level similar to what a near-monopolist like Microsoft does for a product like Word, and the market coverage remaining unusually low despite the presence of multiple vendors.

Mathematically, this negative network effect makes the demand curve convex; see Equation (2). Note that, absent any network effect, it would have been linear, given our assumption of uniformly distributed $u$. As a consequence, the equilibrium price (coverage) in the presence of network effect is larger (smaller), when compared to that in a traditional market (where $g = 0$). Furthermore, this convexity of the demand increases with $g$, which means that price (coverage) increases (decreases) with $g$. Put in plain words, the free-rider problem quickly depresses the demand as the market coverage expands and, therefore, incentivizes the vendors to adopt strategies that reduce the market coverage. Keeping the market coverage low essentially forces consumers to pay substantially for any indirect benefit. The net implication for a security software vendor is, therefore, that negative network effect alters the shape of the demand curve, effectively requiring the strategy of leaving a good part of the market uncovered.

In order to see this more clearly, we plot the equilibrium price, $p^*$, and total market coverage, $nx^*$ in Figure 3. As can be seen from this figure, $p^*$ rises quite rapidly with $g$, whereas the total

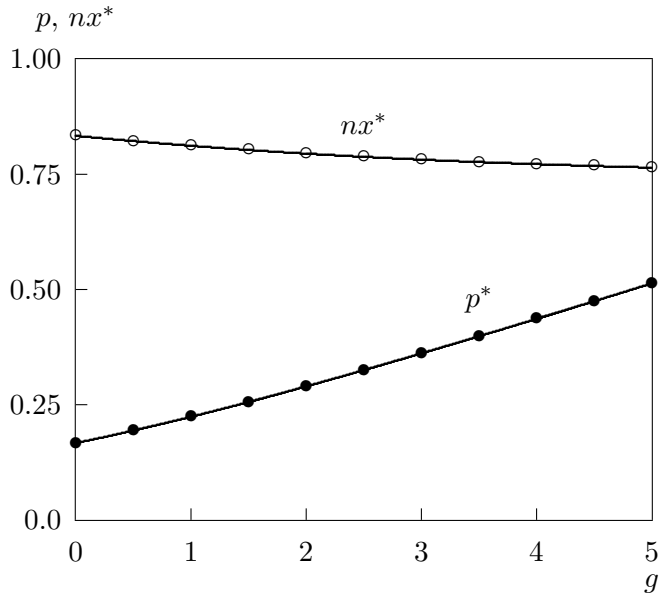



Figure 3: Equilibrium Price and Total Market Coverage, $n = 5$

market coverage, $nx^*$ declines relatively slowly. Consequently, the industry profit, $nx^*p^*$, increases with $g$, i.e., the industry becomes more profitable as the network effect increases. An implication is that, with the world getting more connected and indirect threats increasing, it has become possible for several security software vendors to maintain high prices and make substantial profits while leaving a good part of the market uncovered. Their profitability, however, has attracted other firms to enter the market, an important issue that we discuss next.

### 4.2 Level of Competition

As mentioned earlier, the security software market continues to attract new entrants, in spite of the presence of several major players. Based on our model, we now investigate whether including network effect into the economic framework leads to results consistent with this market characteristic.

We now try to derive the number of vendors operating in this market in equilibrium. In order to incorporate the cost of operating in the security software market, we assume that the marginal cost to the vendor for an additional software subscription is zero. This is a reasonable assumption

since, once the software is developed and updating facilities are established, the marginal cost of supporting an additional subscription in terms of production, distribution, and updating is negligible. Therefore, we only consider the fixed cost incurred by vendors to develop, market, and maintain the software. Since the vendors are all identical, this cost should be the same for all vendors. We use $d$ to denote the *normalized* fixed cost.[7] Clearly, a vendor's incentive compatibility requires her to obtain a revenue no less than this fixed cost. Therefore, if $n^*$ denotes the number of vendors participating in the market in equilibrium, then $R_{\text{olig}}(n^*) \geq d$ and $R_{\text{olig}}(n^*+1) \leq d$. Since $R_{\text{olig}}$ is a decreasing function of $n$, this implies that $n^* = \lfloor \tilde{n} \rfloor$, where $\tilde{n}$ solves:

$$R_{\text{olig}}(\tilde{n}) = p^*_{\text{olig}}(\tilde{n}) x^*_{\text{olig}}(\tilde{n}) = d.$$

Combining this with Corollary 2, we can conclude that, for a given development cost $d$, in equilibrium, the number of vendors in an oligopoly market of security software can be no less than what it would be in the absence of any network effect. In other words, $n^* \geq n^*_0$, where:

$$n^*_0 = \lim_{g \to 0} n^*.$$

Below, we state this more formally:

**Theorem 2.** *Negative network effect leads to a more competitive oligopoly.*

We should mention that, even though we are considering the number of vendors in the market as an indicator for the level of competition, prior literature has proposed other metrics for this purpose, such as the Herfindahl-Hirschman index (Hirschman 1964) and concentration ratio (Adelman 1951). Even when measured against these criteria, we find that negative network effect translates to a higher level of competition.

Theorem 2 indicates that the competitiveness of the security software market can be linked to the presence of negative network effect. Mathematically, for any given market configuration, if $g$ is high, the market coverage is low; but the loss in revenue from this decreased coverage is sufficiently compensated by the high price. The implication is that, just as positive network effect can enhance the profit of a *vendor* in the case of an application software, modest levels of negative network

[7] Recall that we are using a normalized price in the model. Therefore, it is necessary to normalize the fixed cost in the same manner as the price. More specifically, if the absolute fixed cost (per time unit) is $D$, we use $d = D/(\lambda_D L)$.

effect can enhance the *industry* profit in the case of security software. This enhanced profitablity, in turn, can entice new players to enter the market.

In order to illustrate the result in Theorem 2 more clearly, we plot in Figure 4 how the number of vendors, $n^*$, changes with $g$. Two observations can be made from this plot. First, as expected, the number of vendors increases when the fixed cost, $d$, decreases. Second, $n^*$ is a step-wise increasing function of $g$, clearly indicating that the long-run equilibrium competition level increases with negative network effect.

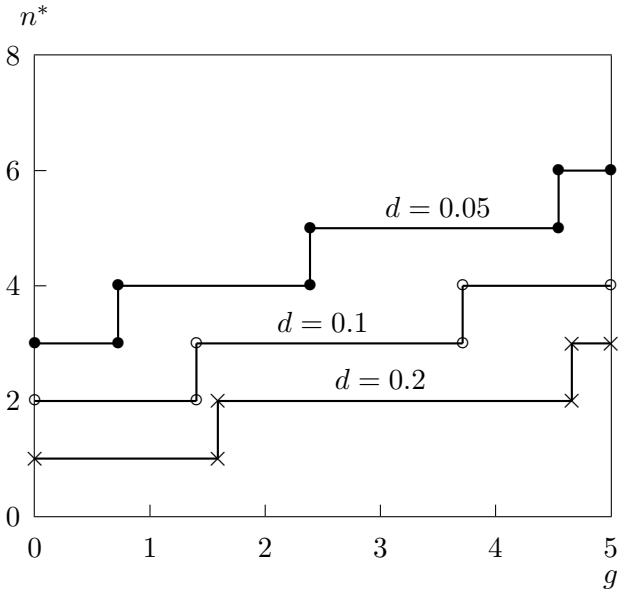



Figure 4: No. of Vendors as a Function of Negative Network Effect

Interestingly, we again find that, when negative network effect is included in the analysis, it becomes much easier to find an explanation as to why this market has remained lucrative to new entrants. With more and more people getting connected with each other through internet or other means, chances of indirect attacks have risen considerably in recent years. In the short run, this has worked against the vendors' incentives to expand coverage and reduce price. However, a lower coverage and higher price together have also meant opportunities for new entrants over the long run.

Although Theorem 2 and Figure 4 are about the long-run equilibrium of the market, their implication must also be noted in terms of how the market is likely to behave during the transitory period—the initial years during which the industry matures. During this transitory phase, vendors

typically make decisions with incomplete information about their own costs, the level of competition, and consumers' reservation prices. A decision-maker must carefully consider the chance of success and profitability before entering the market (Gabszewicz and Thisse 1980, van Herck 1984). If it is believed that the market would be able to support a larger number of vendors, a potential entrant would anticipate a greater chance of succeding. This, in turn, would attract more vendors during the early transitory period—a result quite consistent with the empirical observation by Fosfuri and Giarratana (2004) that the security software market has historically attracted a very large number of vendors, although many of them did not survive beyond the initial years.

### 4.3 New Entry

We now turn our attention to what happens to the price when there is a new entry to the market. In 2006, when Microsoft entered the security software market, there was a large outcry about Microsoft practicing "predatory" pricing to drive out competition (Eckelberry 2006, Keizer 2006). Of course, it is well understood, both in theory and practice, that a new entry is supposed to drive prices down in a traditional market (Gabszewicz and Thisse 1980, Katz and Shapiro 1985, Narasimhan and Zhang 2000). The question we would like to address here is whether the existence of negative network effect makes the new entrant more aggressive and encourages her to reduce the price more drastically when compared to a traditional market.

In order to analyze this in a rigorous manner, we calculate the relative price reduction when a new entrant enters the oligopoly security software market, currently with $n$ players, as:

$$\begin{aligned}\Delta p(n) &= \frac{p^*_{\text{olig}}(n) - p^*_{\text{olig}}(n+1)}{p^*_{\text{olig}}(n)} \\ &= 1 - \frac{(2+n)^2\left(4g(g+1) - (2+n) + (2g+1)\sqrt{4g(g+1)+(2+n)^2}\right)}{(3+n)^2\left(4g(g+1) - (1+n) + (2g+1)\sqrt{4g(g+1)+(1+n)^2}\right)}. \end{aligned} \tag{10}$$

**Theorem 3.** *The relative price reduction resulting from a new entry, $\Delta p(n)$, is an increasing function of negative network effect: $\frac{\partial(\Delta p(n))}{\partial g} \geq 0$, and is bounded: $\frac{1}{2+n} \leq \Delta p(n) \leq \frac{5+2n}{(3+n)^2}$.*

It is clear from Theorem 3 that negative network effect induces a higher reduction in price with a new entry when compared to a traditional market (where $g = 0$). If this is not taken into consideration, the entrant's pricing policy may indeed seem "predatory," as perceived by Eckelberry

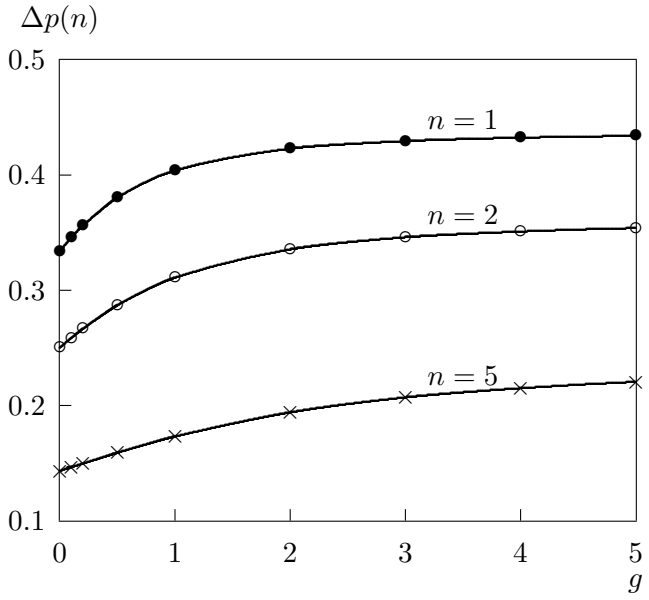



Figure 5: Relative Price Reduction as a Function of Negative Network Effect

(2006). Furthermore, the higher the network effect, the larger is this price reduction. In order to see this more clearly, we plot $\Delta p(n)$ as a function of $g$ in Figure 5. This figure clearly illustrates that the impact of negative network effect on the relative price reduction can be significant. For example, for $n = 2$, $\Delta p(n) = 25\%$ for $g = 0$, but it increases to about 35% for $g = 5$.

## 5 Model Extensions

Although our model provides possible explanations for the unique structure of the security software market, we would like to examine whether these insights are applicable in broader settings. To that end, in this section, we consider two extensions to our basic model by incorporating two additional network effects. The negative network effect that we have examined so far will be called the *type-I effect*, henceforth. Each extension incorporates a new network effect in addition to the type-I effect.

The first extension incorporates a new negative network effect—hereafter called the *type-II effect*—that was identified by Camp and Wolfram (2004), who compare it to that in automotive security, where attempted auto theft, in general, went down when LoJack (an auto theft response system) was first introduced. In the context of information security, this can be formulated in the following manner: Hackers derive utility from breaching security in as many systems as possible.

As more systems adopt security software, this utility goes down. In other words, the motivation of hackers is related to the fraction of the unprotected systems. As this fraction goes down, so does the motivation and, hence, the overall rate of attack. As the rate of attack decreases, the utility to a user from adopting a security software also diminishes.

The second extension, on the other hand, augments the basic model with a positive network effect. The rationale there is as follows: as the fraction of protected users grows, hackers target the unprotected users more and more, leading to an increase in the rate of direct attack for these users. It should be noted that both these effects are recognized in the extant literature; in particular, these effects are closely related to the *choice* and *chance* models of attack on information systems (Ransbotham and Mitra 2009). When the attacks follow a chance model, i.e., when they are opportunistic, their intensity is likely to go down with a higher level of market coverage, as hackers are also utility-maximizing agents (Ransbotham and Mitra 2009). On the other hand, if attacks follow a choice model, then they primarily target vulnerable systems, and the direct attack rate for the unprotected system should increase with a higher level of market coverage. Since, both the attack models exist in the real world, it is necessary to examine both of them.

### 5.1 Type-II Negative Network Effect

We incorporate the type-II effect by making the two attack rates a function of $(1-x)$, the fraction of unprotected systems:

$$\lambda_D = \Lambda_D(1-x)^{r-1} \text{ and } \lambda_I = \Lambda_I(1-x)^{r-1},$$

where $r \geq 1$ denotes the strength of the type-II effect—as $r$ approaches 1, this effect disappears. As before, we let $g = \frac{\lambda_D}{\lambda_I} = \frac{\Lambda_D}{\Lambda_I}$ be the parameter representing the type-I effect. Through simple rearrangement of terms, Equation (2) changes to:

$$p = (1 + g(1-x))\,(1-x)^r. \tag{11}$$

**Monopoly Market**

The monopolist, in this case, would want to solve the following optimization problem:

$$\underset{x_{\text{mon}}}{\text{Max}}\, R_{\text{mon}} = p_{\text{mon}} x_{\text{mon}} = (1 + g(1 - x_{\text{mon}}))(1 - x_{\text{mon}})^r x_{\text{mon}};\ 0 \leq x_{\text{mon}} \leq 1. \tag{12}$$

We can easily solve (12) for the following result:

**Proposition 3.** *In the monopoly market where both type-I and type-II effects are present, the optimal market share and price are given by:*

$$x^*_{\text{mon}} = \frac{g(r+3) + r + 1 - \sqrt{(r+1)^2(g+1)^2 - 4g}}{2g(r+2)} \text{ and} \tag{13}$$

$$p^*_{\text{mon}} = \left(\frac{(g-1)(r+1) + \sqrt{(r+1)^2(1+g)^2 - 4g}}{2g(r+2)}\right)^r \times \left(\frac{g(r+1)+r+3+\sqrt{(r+1)^2(1+g)^2 - 4g}}{2(r+2)}\right). \tag{14}$$

By taking limits of these expressions as $r \to 1$, it can be shown that Proposition 3 converges to Proposition 1.

**Oligopoly Market**

As before, we assume that, in equilibrium, there are $n$ identical vendors in the market with non-negative revenue. The aggregate market size is once again $M$, where $M = \sum_{i=1}^{n} x_i$, and $x_i$ is vendor $i$'s market size. We denote $\sum x_{-i} = M - x_i$. Since the vendors are identical, the prices set by them are all equal to $(1+g(1-M))(1-M)^r$ from (11). For vendor $i$, the revenue maximization problem becomes:

$$\underset{x_i}{\text{Max}}\, R_{\text{olig}} = \left(1 + g\left(1 - \sum x_{-i} - x_i\right)\right)\left(1 - \sum x_{-i} - x_i\right)^r x_i;\ \ 0 \leq \sum_{i=1}^{n} x_i \leq 1. \tag{15}$$

Solving (15), the following result is obtained:

**Proposition 4.** *In the oligopoly market with n identical vendors, where both type-I and type-II*

*effects are present, the equilibrium market size and price for each vendor are given by:*

$$x^*_{\text{olig}} = \frac{g(r+2n+1)+r+n-\sqrt{(g+n+r(g+1))^2-4gn}}{2gn(r+n+1)} \text{ and} \tag{16}$$

$$p^*_{\text{olig}} = \left(\frac{g(r+1)-r-n+\sqrt{(g+n+r(1+g))^2-4gn}}{2g(r+n+1)}\right)^r \times \left(\frac{g(r+1)+r+n+2+\sqrt{(g+n+r(1+g))^2-4gn}}{2(r+n+1)}\right). \tag{17}$$

Once again, by taking the limit of each of the above two expressions as $r \to 1$, it can be shown that the results in Proposition 4 converge to those in Proposition 2.

**Corollary 3.** *The oligopoly market with both type-I and type-II effects has the following characteristics:*

(i) $\dfrac{\partial x^*_{\text{olig}}}{\partial g} \le 0,\ \dfrac{\partial x^*_{\text{olig}}}{\partial r} \le 0,\ \text{and}\ \dfrac{\partial x^*_{\text{olig}}}{\partial n} \le 0.$

(ii) $\dfrac{\partial p^*_{\text{olig}}}{\partial g} \ge 0,\ \dfrac{\partial p^*_{\text{olig}}}{\partial r} \le 0,\ \text{and}\ \dfrac{\partial p^*_{\text{olig}}}{\partial n} \le 0.$

(iii) $\dfrac{\partial R_{\text{olig}}\left(x^*_{\text{olig}}\right)}{\partial g} \ge 0,\ \dfrac{\partial R_{\text{olig}}\left(x^*_{\text{olig}}\right)}{\partial r} \le 0,\ \text{and}\ \dfrac{\partial R_{\text{olig}}\left(x^*_{\text{olig}}\right)}{\partial n} \le 0.$

Corollary 3 is basically an extension of Corollary 2. Therefore, as before, Corollary 3 indicates that, even in the presence of the type-II effect, the impact of the type-I effect is similar to what we have described earlier (see Corollary 2)—a large $g$ still means a low market coverage and a high price. The new result from Corollary 3 is, therefore, about the impact of the type-II effect. We find that a more pronounced type-II effect (i.e., a larger $r$) would lead to a smaller market share as well as a lower price.

**Theorem 4.** *Even in the presence of the type-II effect, the type-I effect leads to a more competitive market. However, the type-II effect leads to a less competitive market.*

The first part of Theorem 4 makes it clear that our earlier insights regarding the type-I effect (see Theorem 2) remains valid in a wider context, further strengthening our intuition that modest levels of it can explain the market structure for security software. The second part provides us with an additional insight: Not all negative network effects are the same. Their impacts depend on how they manifest themselves in a specific market. Though the type-II effect furnishes some

support for the low market coverage commonly observed, it does not lend any support to other market characteristics, namely its fragmented nature.

In order to understand why the type-II effect manifests itself differently, we first note that it exacerbates the free-rider problem present with the type-I effect, making the WTP even lower. When the type-II effect is present, the optimal strategy for vendors is to cover even less market, i.e., $\frac{\partial x^*_{\text{olig}}}{\partial r} \leq 0$, because a steeper reduction in the market coverage is necessary to contain the amplified free-rider problem. However, because the WTP in this case declines very fast with $r$, it becomes harder for the vendors to maintain high price levels. In fact, the equilibrium price also declines with $r$, i.e., $\frac{\partial p^*_{\text{olig}}}{\partial r} \leq 0$. Evidently, it is no longer possible to compensate for the lower market coverage by hiking the price. The end result is that the industry profit is also decreasing in $r$, implying that the type-II effect makes the market incapable of sustaining as many players as the market can in its absence.

### 5.2 Positive Network Effect

In order to capture the network effect resulting from increased direct attack on unprotected systems (or any other factor not explicitly considered), we can simply set the rate of direct attacks to $\lambda_D x$, where, $x$, as before, is the market coverage. The total benefit per unit time to user $u$ then changes to:

$$B_u = \lambda_D x L u + \lambda_I (1-x) L u = \lambda_D L u \left(x + g(1-x)\right).$$

Once again, considering the marginal user who is indifferent between adopting and not adopting, we can find the normalized demand equation as:

$$p = \left(x + g(1-x)\right)(1-x). \tag{18}$$

A closer examination of Equation (18) reveals that this extended model captures both positive and negative network effects. To see this clearly, note that the term $(x + g(1-x))$ has two parts: (i) $x$, which increases the WTP as the market coverage increases, and (ii) $g(1-x)$, which is the type-I effect. Interestingly, this can be seen another way by rearranging the term $(x + g(1-x))$ in the

expression for the WTP of the marginal user:

$$p = (1 + (g-1)(1-x))\,(1-x). \tag{19}$$

Comparing Equation (19) to Equation (2), we note that they are exactly the same, the only difference being that $g$ in Equation (2) is now replaced with $(g-1)$; here, the term $(g-1)$ parameterizes the overall network effect. When $0 < g < 1$, the net effect is positive in nature, i.e., positive network effect dominates. In contrast, the overall effect is negative when $g > 1$—in this case, negative network effect dominates. At $g = 1$, there is no network effect, and we end up with the traditional market. In order to see this more clearly, we define $h = -\ln(g)$ as the *network effect parameter*; as shown in Figure 6, when $h = 0$, there is no network effect, and the total network effect is positive (negative) if $h$ is positive (negative).

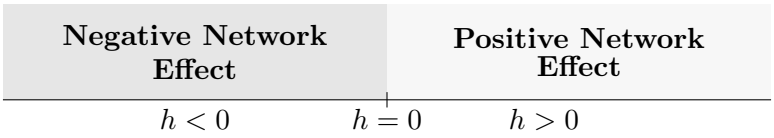
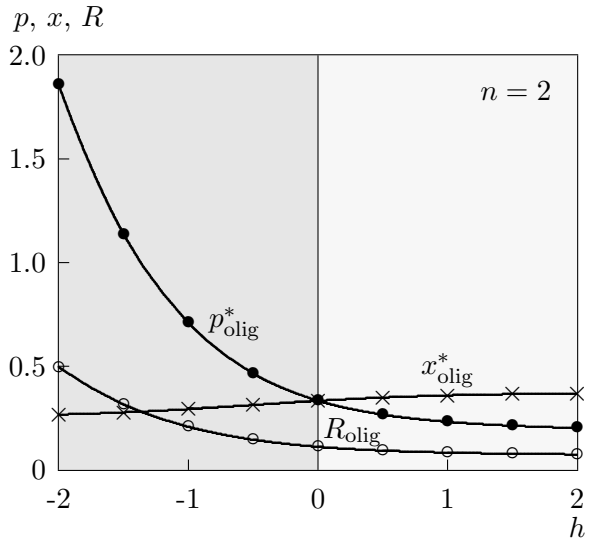


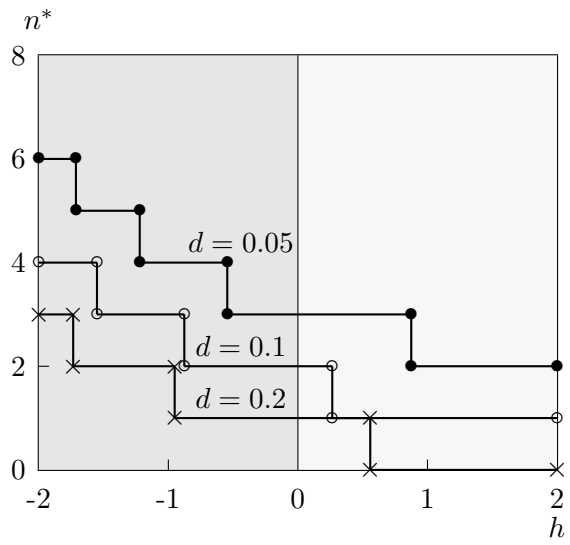

Figure 6: Market Condition Based on Network Effect Parameter

**Theorem 5.** *In the presence of both the positive and type-I negative network effects, all the results in Sections 3 and 4 hold, provided $g$ is replaced with $(g-1)$ in them.*

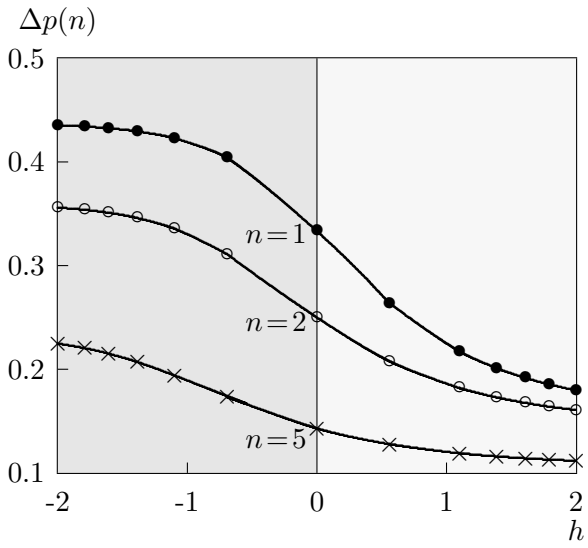
This extended model thus provides a more complete picture of the market since, using just one parameter, it captures both positive and negative network effects. In Figure 7, we plot some of the interesting results in this paper as a function of $h$, the network effect parameter. As can be seen from figure, in the darker region ($h < 0$), our results exhibit the same characteristics as before. However, in the lighter region ($h > 0$), we now have the results for the case where the positive network effect prevails. Not surprisingly, these results are akin to what we already know about typical software markets, where the positive network effect has a much stronger influence. For example, as $h$ increases, the market coverage increases, the price goes down, and the number of vendors reduces. Furthermore, the relative change in price due to a new entry into the market is much smaller when $h > 0$.




(a) Price, Market Coverage, and Revenue




(b) No. of Vendors




(c) Price Reduction

Figure 7: Market Structure under Positive and Negative Network Effects

## 6 Conclusions and Future Directions

A security software is a tool that individuals and organizations deploy to prevent security exploitations of computerized systems. Over the last decade, the market for this type of software has seen a tremendous growth, both from the supply as well as the demand side. Unlike the typical software market, where the supply side is dominated by only a handful of providers, the market for security software is highly competitive with several major players. In this paper, we search for possible explanations as to why the security software market behaves differently from the other ones.

The positive network effect enjoyed by other software is not usually observed for security software; this is because the compatibility issue of application data across users is not a big concern. On the contrary, there is a negative network effect for security software—as the market coverage declines, the chance of an indirect attack from an unprotected computer increases. Though prior research has looked at this negative network effect in the context of application software security and patching (August and Tunca 2006, 2008, 2011), we are the first to study its possible impacts on the security software market. We make the case that most of the idiosyncrasies and prevailing conditions in this market can be explained by this negative network effect.

More specifically, we find that negative network effect leads to a free-rider problem, resulting in lower equilibrium market coverage and higher prices, both in monopoly and oligopoly settings. The implication for vendors of security software is that, when negative network effect is present, it is optimal to use strategies that keep the total market coverage low. Otherwise, an excessive amount of free-riding would occur, adversely affecting the pricing power and profitability. We also find that, by keeping the coverage low and charging consumers substantial amounts for indirect benefits, the vendors can actually profit from this network effect. Acknowledging the role of negative network effect thus makes it a lot more easier to explain why the industry is so profitable despite unusually low market coverage. Further, any higher profitability in the short run also means that, for any given fixed entry cost, there would be more firms entering the market in the long run. Intriguingly, all these observations are in line with the realities of the security software market. First of all, despite an insignificant marginal cost, a two-year subscription of antivirus software made by Trend Micro or Kaspersky can cost an amount that is comparable to the cost of Microsoft Word 2010, a product that enjoys near monopoly power. Furthermore, there are dozens of vendors in the market for third-party security software, which is far more than what is seen in most other markets.

We also find that negative network effect is likely to make new entrants more aggressive when compared to a traditional market. Perhaps, this explains why Microsoft—a late entrant in this market—priced its *OneCare* software at a level that, in 2006, was deemed "predatory" by many contemporary commentators (Eckelberry 2006, Keizer 2006). This result also points to the fact that incorporating negative network effect into economic models may be an useful exercise for researchers and practitioners interested in understanding the unique structure of the security software market.

In order to verify the applicability of our insights to different possible contexts, we carefully

extend our analysis to different forms of network effects. One extension considers the fact that hackers are likely to step up attack rates when there are large number of insecure machines around. We find that allowing such variable attack rates does not affect our earlier results pertaining to equilibrium prices and coverage, although the variability manifests itself somewhat differently. A second extension looks at the possibility that hackers may target vulnerable machines to maximize their chances of succeeding. This extension essentially leads to a scenario where both positive and negative network effects are present. We show that, so long as the negative network effect remains the dominant component, all our earlier results carry over.

In conclusion, we find a reasonable analytical support for the possibility that negative network effect can explain the idiosyncratic nature of the security software market. Our analysis also makes it clear how vendors in this fiercely competitive market may adjust their strategic decisions depending on different network effects. There are several directions in which our results can be extended. For example, we have assumed that the level of negative network effect, $g$, is the same for all consumers though it might vary across individual users or organizations, depending on how they deploy complementary security technologies, such as firewalls and intrusion prevention systems. Further, nonlinear pricing through volume licensing is common in many software markets (Sundararajan 2004). One could investigate how nonlinear pricing might help security software vendors leverage network effects. In addition, our model of a symmetric competitive equilibrium can be extended to asymmetric settings. We are examining some of these issues in our ongoing efforts.

## References


Adelman, M. A. 1951. The measurement of industrial concentration. *The Review of Economics and Statistics* **33**(4) 269–296.

Anderson, J. 2001. Why information security is hard—an economic perspective. *Proceedings of the Seventeenth Computer Security Applications Conference* 358–365.

Anderson, R., T. Moore. 2006. The economics of information security. *Science* **314**(5799) 610–613.

August, T., T. I. Tunca. 2006. Network software security and user incentives. *Management Science* **52**(11) 1703–1720.

August, T., T. I. Tunca. 2008. Let the pirates patch? An economic analysis of software security patch restrictions. *Information Systems Research* **19**(1) 48–70.

August, T., T. I. Tunca. 2011. Who should be responsible for software security? A comparative analysis of liability policies in network environments. *Management Science* **57**(5) 934–959.

Basu, A., T. Mazumdar, S. P. Raj. 2003. Indirect network externality effects on product attributes. *Marketing Science* **22**(2) 209–221.

Böhme, R. 2005. Cyber-insurance revisited. *4th Workshop on the Economics of Information Security* .

Braverman, M. 2005. Blaster: A case study from Microsoft's perspective. *Virus Bulletin Conference* 200–205.

Brynjolfsson, E., C. Kemerer. 1996. Network externalities in microcomputer software: An econometric analysis of the spreadsheet market. *Management Science* **42**(12) 1627–1647.

Camp, L. J., C. Wolfram. 2004. Pricing Security. *Economics of Information Security, L. J. Camp and S. Lewis (Eds.)*. Springer.

Chen, P., G. Kataria, R. Krishnan. 2005. Software diversity for information security. *4th Workshop on the Economics of Information Security* .

Eckelberry, A. 2006. Microsoft practices predatory pricing. *Sunbeltblog* URL `http://sunbeltblog.blogspot.com/2006/06/microsoft-practices-predatory-pricing.html`.

Economides, N. 1996. Network externalities, complementarities and invitations to enter. *European Journal of Political Economy* **12**(2) 211–233.

Eichorn, K., J. Smith. 2011. McAfee releases online banking safety guide for the 47 percent of consumers who are underprotected. *McAfee Press Release* URL `http://www.mcafee.com/us/about/news/2011/q3/20110803-01.aspx`.

Farrell, J., G. Saloner. 1986. Installed base and compatibility: Innovation, product preannouncements, and predation. *American Economic Review* **76**(5) 940–955.

Fosfuri, A., M. S. Giarratana. 2004. Product strategies and startups' survival in turbulent industries: Evidence from the security software industry. *Working Paper* (Universidad Carlos III de Madrid).

Gabszewicz, J. J., J.-F. Thisse. 1980. Entry (and exit) in a differentiated industry. *Journal of Economic Theory* **22**(2) 327–338.

Gal-Or, E., A. Ghose. 2003. The economic consequences of sharing security information. *2nd Workshop on the Economics of Information Security* .

Gandal, N. 1995. Competing compatibility standards and network externalities in the PC software market. *Journal of Economic Theory* **77**(4) 599–608.

Ghose, A., A. Sundararajan. 2005. Pricing security software: Theory and evidence. *4th Workshop on the Economics of Information Security* .

Giarratana, S. M. 2004. The birth of a new industry: Entry by start-ups and the drivers of vendor growth: The case of encryption software. *Research Policy* **33**(5) 787–806.

Goodchild, J. 2011. Botnets: Size isn't everything, says new report. *Computerworld* URL `http://news.idg.no/cw/art.cfm?id=E795F760-1A64-6A71-CEE2E437E7955007`.

Gordon, L. A., M. P. Loeb. 2002. The economics of information security investment. *ACM Transactions on Information and System Security* **5**(4) 438–457.

Gordon, L. A., M. P. Loeb. 2006. Budgeting process for information security expenditures. *Communications of the ACM* **49**(10) 121–125.

Gordon, L. A., M. P. Loeb, W. Lucyshyn. 2003. Sharing information on computer systems: An economic analysis. *Journal of Accounting and Public Policy* **22**(6) 461–485.

Grillo, I., O. Shy, J.-F. Thisse. 2001. Price competition when consumer behavior is characterized by conformity or vanity. *Journal of Public Economics* **80** 385–408.

Hirschman, A. O. 1964. The paternity of an index. *American Economic Review* **54**(5) 761–762.

Hotelling, H. 1929. Stability in competition. *The Economic Journal* **39**(153) 41–57.

Kannan, K., R. Telang. 2005. Market for software vulnerabilities? Think again. *Management Science* **51**(5) 726–740.

Katz, M. L., C. Shapiro. 1985. Network externalities, competition and compatibility. *American Economic Review* **75**(3) 424–440.

Katz, M. L., C. Shapiro. 1986. Technology adoption in the presence of network externalities. *Journal of Political Economy* **94**(4) 822–841.

Keizer, G. 2006. Rival calls Microsoft's security pricing 'predatory,' 'ruthless'. *Techweb Network* URL `http://www.techweb.com/showArticle.jhtml?articleID=189600266`.

Kreps, D. M., J. A. Scheinkman. 1983. Quantity precommitment and Bertrand competition yield Cournot outcomes. *The Bell Journal of Economics* **14**(2) 326–337.

Lacy, S. 2006. Microsoft sweeps into security. *Business Week* URL `http://www.businessweek.com/technology/content/may2006/tc20060531_497986.htm`.

Latimer-Livingston, N. S., R. Contu. 2007. Forecast: Security software worldwide, 2006–2011, update. *Gartner Report* URL `http://www.gartner.com/DisplayDocument?ref=g_search&id=510567&subref=sim`.

Leibenstein, H. 1950. Bandwagon, snob and veblen effects in the theory of consumers' demand. *The Quarterly Journal of Economics* **64**(2) 183–207.

Liebowitz, S. J., E. S. Margolis. 1999. Cause and consequences of market leadership in application software. *Conference of Competition and Innovation in the Personal Computer Industry* .

Low, W., D. Chung. 2006. Asia/Pacific (excluding Japan) security software 2006—2010 forecast and analysis. *IDC Report* URL `http://www.idc.com/getdoc.jsp?containerId=AP322306N`.

McCormack, K. 2006. Enterprise software's growth pocket. (an interview of S&P's Zaineb Bokhari by Karyn McCormack). *Business Week* URL `http://www.businessweek.com/investor/content/may2006/pi20060524_164054.htm`.

Narasimhan, C., Z. Zhang. 2000. Market entry strategy under firm heterogeneity and asymmetric payoffs. *Marketing Science* **19**(4) 313–327.

Ogut, H., N. Menon, S. Raghunathan. 2005. Cyber insurance and IT security investment: Impact of interdependent risk. *4th Workshop on the Economics of Information Security* .

Png, I. P. L., C. Q. Tang, Q. Wang. 2006. Hackers, users, information security. *5th Workshop on the Economics of Information Security* .

Ransbotham, S., S. Mitra. 2009. Choice and chance: A concepual model of paths to information security compromise. *Information Systems Research* **20**(1) 121–139.

Salop, S. C. 1979. Monopolistic competition with outside goods. *The Bell Journal of Economics* **10**(1) 141–156.

Sancho, D. 2005. The future of BOT worms. *Trend Micro White Paper* URL `http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/future_of_bots_final.pdf`.

Shapiro, C., H. R. Varian. 1999. *Information Rules: A Strategic Guide to the Network Economy*. Boston: Harvard Business School Press.

Sundararajan, A. 2004. Nonlinear pricing of information goods. *Management Science* **50**(12) 1660–1673.

van Herck, G. 1984. Entry, exit and profitability. *Managerial and Decision Economics* **5**(1) 25–31.

Varian, H. R. 2000. Managing online security risks. *The New York Times* URL `http://www.nytimes.com/library/financial/columns/060100econ-scene.html`.

Zhang, Z., D. Dey, Y. Tan. 2007. Pricing communication services with delay guarantee. *INFORMS Journal on Computing* **19**(2) 248–260.

# Appendix

# A Proofs

## Proof of Proposition 1

The first order condition — $\frac{dR_{\text{mon}}}{dx_{\text{mon}}} = 1 - 2x_{\text{mon}} + g(1 - x_{\text{mon}})(1 - 3x_{\text{mon}}) = 0$— can be solved to obtain (5). Substituting (5) into (3), we get (6). Furthermore, $\frac{d^2R_{\text{mon}}}{dx^2_{\text{mon}}} = -2 - 2g(2 - 3x^*_{\text{mon}})$. Since $x^*_{\text{mon}} \leq \frac{1}{2}$ (from Corollary 1), $\frac{d^2R_{\text{mon}}}{dx^2_{\text{mon}}} < 0$. In other words, the second order condition is also satisfied. ■

## Proof of Corollary 1

We need to show that:

$$x^*_{\text{mon}} \leq \frac{1}{2},\ p^*_{\text{mon}} \geq \frac{1}{2},\ \text{and}\ R_{\text{mon}}(x^*_{\text{mon}}) \geq \frac{1}{4}.$$

First, we see that

$$x^*_{\text{mon}} - \frac{1}{2} = \frac{(2g+1) - \sqrt{g^2+g+1}}{3g} - \frac{1}{2} = \frac{(\frac{g}{2}+1) - \sqrt{g^2+g+1}}{3g}.$$

Since $\sqrt{g^2+g+1} \geq \sqrt{\frac{g^2}{4}+g+1} = \frac{g}{2}+1$, we conclude that $x^*_{\text{mon}} \leq \frac{1}{2}$. Next,

$$p^*_{\text{mon}} = (1 + g(1 - x^*_{\text{mon}}))(1 - x^*_{\text{mon}}) \geq 1 - x^*_{\text{mon}} \geq \frac{1}{2}.$$

Finally,

$$R_{\text{mon}}(x^*_{\text{mon}}) - \frac{1}{4} = p^*_{\text{mon}}x^*_{\text{mon}} - \frac{1}{4} = \frac{2(g^2+g+1)^{1.5} - (3.75g^2+3g+2)}{27g^3}.$$

Let $A = 2(g^2+g+1)^{1.5}$ and $B = 3.75g^2+3g+2$. Then $A^2 - B^2 = 4g^6 + 12g^5 + 9.9375g^4 + 5.5g^3 \geq 0$. Therefore, $A \geq B$ and $R_{\text{mon}}(x^*_{\text{mon}}) \geq \frac{1}{4}$. ■

## Proof of Proposition 2

The first order condition is:

$$\frac{\partial R_{\text{olig}}}{\partial x_i} = \left(1 - \sum x_{-i} - 2x_i\right) + g\left(1 - \sum x_{-i} - x_i\right)\left(1 - \sum x_{-i} - 3x_i\right) = 0. \tag{A1}$$

This results in a quadratic equation in $x_i$. We solve this equation, with the restriction that $0 \leq \sum_{i=1}^{n} x_i \leq 1$, to get:

$$x_i = \frac{1 + 2g - 2g\sum x_{-i} - \sqrt{1+g+g^2-(g+2g^2)\sum x_{-i} + g^2\left(\sum x_{-i}\right)^2}}{3g}. \tag{A2}$$

Since the vendors are identical, we consider only the symmetric equilibrium, i.e., $x_i$'s are all equal, as are the corresponding $p_i$'s. Let $x_i = x_{\text{olig}}$ and $p_i = p_{\text{olig}}$. In that case, $\sum x_{-i} = (n-1)x_{\text{olig}}$. Plugging this back into (A2) and solving for $x_{\text{olig}}$, we get (8). The equilibrium price is then given by:

$$\begin{aligned} p^*_{\text{olig}} &= \left(1 + g\left(1 - nx^*_{\text{olig}}\right)\right)\left(1 - nx^*_{\text{olig}}\right) \\ &= \frac{4g(g+1) - (1+n) + (2g+1)\sqrt{4g(g+1)+(1+n)^2}}{2g(2+n)^2}. \end{aligned}$$

Finally, we need to verify whether the second order condition is satisfied, i.e., whether:

$$\frac{\partial^2 R_{\text{olig}}}{\partial x_i^2} = -2\left(1 + gx_i + 2g\left(1 - \sum x_{-i} - 2x_i\right)\right) < 0.$$

In order to complete the proof then, we must show that $1-\sum x_{-i}-2x_i>0$. Suppose this is not true, i.e., $1-\sum x_{-i}-2x_i\leq 0$. Since $x_i\geq 0$, this implies that $1-\sum x_{-i}-3x_i<0$. Furthermore, since $\sum_{i=1}^{n} x_i\leq 1$, we have $1-\sum x_{-i}-x_i>0$. Therefore, the expression

$$\left(1-\sum x_{-i}-2x_i\right)+g\left(1-\sum x_{-i}-x_i\right)\left(1-\sum x_{-i}-3x_i\right)$$

is negative, which contradicts the first order condition in (A1). ■

## Proof of Corollary 2

Taking partial derivatives of $x^*_{\text{olig}}$ and $p^*_{\text{olig}}$ with respect to $g$ and $n$, and rearranging terms, we get:

$$\begin{aligned}
\frac{\partial x^*_{\text{olig}}}{\partial g} &= \frac{2g+(1+n)^2-(1+n)\sqrt{4g(g+1)+(1+n)^2}}{2g^2n(2+n)\sqrt{4g(g+1)+(1+n)^2}},\\
\frac{\partial x^*_{\text{olig}}}{\partial n} &= \frac{-(1+2g)(2+n(2+n))\sqrt{4g(1+g)+(1+n)^2}+(1+n)(2+8g(1+g)+n(2+n))}{2gn^2(2+n)^2\sqrt{4g(g+1)+(1+n)^2}},\\
\frac{\partial p^*_{\text{olig}}}{\partial g} &= \frac{-(1+2g-4g^2-8g^3+2n+n^2)+\left(1+4g^2+n\right)\sqrt{4g(g+1)+(1+n)^2}}{2g^2(2+n)^2\sqrt{4g(g+1)+(1+n)^2}}, \text{ and}\\
\frac{\partial p^*_{\text{olig}}}{\partial n} &= \frac{-(2g+1)\left(8g(g+1)+n+n^2\right)+(-8g(g+1)+n)\sqrt{4g(g+1)+(1+n)^2}}{2g(2+n)^3\sqrt{4g(g+1)+(1+n)^2}}.
\end{aligned}$$

To find the sign of the first expression, we set $A=(1+n)\sqrt{4g(g+1)+(1+n)^2}$ and $B=2g+(1+n)^2$. Since $A^2-B^2=4g^2n(2+n)\geq 0$, $A\leq B$ and, hence, $\frac{\partial x^*_{\text{olig}}}{\partial g}\leq 0$. To prove that the second expression is negative, let $A=(2g+1)(2+2n+n^2)\sqrt{4g(g+1)+(1+n)^2}$ and $B=(1+n)(2+8g(g+1)+n(2+n))$. After some algebraic manipulations, it can be shown that: $A^2-B^2=4g(g+1)n^2(2+n)^2(2+4g(g+1)+n(2+n))\geq 0$, implying $A\geq B$ and hence $\frac{\partial x^*_{\text{olig}}}{\partial n}\leq 0$.

In order to examine the sign of the third expression, we set $A=1+2g-4g^2-8g^3+2n+n^2$ and $B=\left(1+4g^2+n\right)\sqrt{4g(g+1)+(1+n)^2}$. It is clear that $B>0$. Therefore, if $A\leq 0$, $B\geq A$, trivially. On the other hand, if $A>0$, we find that: $B^2-A^2=4g^2(2+n)^2\left((1+2g)^2+2n\right)\geq 0$, which implies that $B\geq A$ and $\frac{\partial p^*_{\text{olig}}}{\partial g}\geq 0$. Finally, to prove the last expression, we set: $A=(2g+1)(8g(g+1)+n+n^2)$ and $B=(-8g(g+1)+n)\sqrt{4g(g+1)+(1+n)^2}$. In this case, $A>0$. So, if $B\leq 0$, $A>B$ holds trivially. If, however, $B>0$, then $A^2-B^2=4g(g+1)n(2+n)^3\geq 0$, which implies that $A\geq B$ and, hence, $\frac{\partial p^*_{\text{olig}}}{\partial n}\leq 0$.

Next, we know that $R_{\text{olig}}\left(x^*_{\text{olig}}\right)=p^*_{\text{olig}}x^*_{\text{olig}}$. Taking a partial derivative with respect to $g$ and simplifying, we can write:

$$\frac{\partial R_{\text{olig}}\left(x^*_{\text{olig}}\right)}{\partial g}=\frac{A-B}{g^3n(2+n)^3\sqrt{4g(g+1)+(1+n)^2}},$$

where

$$\begin{aligned}
A &= \left((g+1)(1+n^2)+n(2+g+2g^3)\right)\sqrt{4g(g+1)+(1+n)^2} \text{ and}\\
B &= (1+3g+2g^2)+n(3+4g+4g^2-2g^3-4g^4)+n^2(3+2g)+n^3(g+1).
\end{aligned}$$

In order to complete the proof, we have to show $A\geq B$. If $B\leq 0$, this is obvious. Therefore, let us consider the case where $B>0$. In that case also, $A\geq B$, since

$$A^2-B^2=4g^2(g+1)n(2+n)^3(g(g+1)+n)\geq 0.$$

Lastly, we know:

$$\frac{\partial R_{\text{olig}}\left(x^*_{\text{olig}}\right)}{\partial n}=p^*_{\text{olig}}\frac{\partial x^*_{\text{olig}}}{\partial n}+x^*_{\text{olig}}\frac{\partial p^*_{\text{olig}}}{\partial n}.$$

Since $p^*_{\text{olig}} > 0$, $x^*_{\text{olig}} > 0$, $\frac{\partial x^*_{\text{olig}}}{\partial n} \leq 0$, and $\frac{\partial p^*_{\text{olig}}}{\partial n} \leq 0$, it is clear that $\frac{\partial R_{\text{olig}}\left(x^*_{\text{olig}}\right)}{\partial n} \leq 0$. ■

## Proof of Theorem 1

Straightforward from Corollary 2. ■

## Proof of Theorem 2

The equilibrium market coverage and price for a traditional oligopoly market (without the negative network effect) are both $\frac{1}{n+1}$, resulting in a total revenue of $\frac{1}{(n+1)^2}$.

We know that:

$$\lim_{g\to 0} R_{\text{olig}}(x^*_{\text{olig}}) = \frac{1}{(n+1)^2}.$$

Furthermore, from Corollary 2, we have $\frac{\partial R_{\text{olig}}\left(x^*_{\text{olig}}\right)}{\partial g} \geq 0$. Combining these two facts, it is clear that the revenue in our case is strictly greater than that in a traditional oligopoly. Since the revenue is also a decreasing function of $n$ (see Corollary 2), given a development cost, the number of vendors in this setting cannot be less than that in a traditional oligopoly, i.e., $n^* \geq n^*_0$. ■

## Proof of Theorem 3

Let $F = \sqrt{4g(g+1)+(1+n)^2}$ and $G = \sqrt{4g(g+1)+(2+n)^2}$. Then, to prove the first part, we take partial derivative of $\Delta p(n)$ in (10) with respect to $g$. After some algebraic manipulations, we find that:

$$\frac{\partial(\Delta p(n))}{\partial g} = C(A-B),$$

where

$$\begin{aligned} A &= (1+2g)^3(3+2n) + F\left(13+17n+7n^2+n^3+4g(1+g)(7+6n+n^2)\right), \\ B &= G\left(2F(1+2g) + \left(6+10n+6n^2+n^3+4g(1+g)(6+4n+n^2)\right)\right), \text{ and} \\ C &= \frac{2(2+n)^2}{FG\left[(3+n)\left(1+n-4g(1+g)-F(1+2g)\right)\right]^2}. \end{aligned}$$

Since, $C > 0$, we only need to show that $A \geq B$. We find that:

$$A^2 - B^2 = 2(3+n)^2\left((2g+1)^2 + 4n(1+2g+2g^2) + 2n^2\right)(X-Y),$$

where $X = (1+n)^2 + 16g^2(1+g)^2 + 2gn^2(1+g)$ and $Y = F(1+2g)((1+n)-4g(1+g))$. It turns out that $X^2 - Y^2 = 4g^2(1+g)^2(2+n)^4 \geq 0$, so $X \geq Y$ and, hence, $A \geq B$.

Since $\Delta p(n)$ is a monotonic function of $g$, to prove that $\Delta p(n)$ is bounded, simply note that $\lim_{g\to 0} \Delta p(n) = \frac{1}{2+n}$ and $\lim_{g\to\infty} \Delta p(n) = \frac{5+2n}{(3+n)^2}$. ■

## Proof of Proposition 3

The first order condition:

$$\frac{dR_{\text{mon}}}{dx_{\text{mon}}} = (1-x_{\text{mon}})^{r-1}\left(1-x_{\text{mon}}(r+1) + g\left(1-x_{\text{mon}}\right)\left(1-(r+2)x_{\text{mon}}\right)\right) = 0$$

can be solved to obtain $x^*_{\text{mon}}$ in (13), which, in turn, can be substituted into the expression for $p_{\text{mon}}$ to obtain (14). Since

$$\frac{d^2R_{\text{mon}}}{dx^2_{\text{mon}}} = (1-x_{\text{mon}})^{r-2}\left(\left(2-x_{\text{mon}}(r+1)\right)r + g(1+r)\left(1-x_{\text{mon}}\right)\left(2-(r+2)x_{\text{mon}}\right)\right) < 0$$

when $x_{\text{mon}} = x^*_{\text{mon}}$, the second order condition is also satisfied. ■

## Proof of Proposition 4

Let $X_i = \sum x_{-i}$. The first order condition for (15) can then be written as:

$$\frac{dR_{\text{olig}}}{dx_i} = (1 - X_i - x_i)^{r-1} \left(1 - X_i - x_i(r+1) + g\left(1 - X_i - x_i\right)\left(1 - X_i - x_i(r+2)\right)\right) = 0.$$

This results in a quadratic equation in $x_i$, which can solved, with the following restrictions: $0 \leq \sum_{i=1}^{n} x_i \leq 1$, $x_i = x_{\text{olig}}$, and $X_i = (n-1)x_{\text{olig}}$ to obtain (16). Then, $x_{\text{olig}}$ can be substituted into $p^*_{\text{olig}} = (1 + g(1 - nx^*_{\text{olig}}))(1 - nx^*_{\text{olig}})^r$ to obtain the equilibrium price given by (17). We now consider the second order condition. After some effort, we can show that:

$$\frac{d^2 R_{\text{olig}}}{dx_i^2} = -\left(1-X_i-x_i\right)^{r-2}\left(r\left(2-2X_i-x_i(r+1)\right) + g(r+1)\left(1-X_i-x_i\right)\left(2-2X_i-x_i(r+2)\right)\right).$$

Now, since $1–X_i–x_i > 0$, $\frac{d^2 R_{\text{olig}}}{dx_i^2} < 0$ if $2–2X_i–x_i(r+2) > 0$. Suppose this is not true, i.e., $2–2X_i–x_i(r+2) \leq 0$. This also means $1-X_i-x_i(r+2) < 0$. However, that is not possible since it implies $\frac{dR_{\text{olig}}}{dx_i} < 0$—a violation of the first order condition. ■

## Proof of Corollary 3

With some algebra, we can show that:

$$\frac{\partial x^*_{\text{olig}}}{\partial g} = \frac{g(n(r-1)+r(r+1)) + (r+n)^2 - (r+n)\sqrt{(g+n+r(g+1))^2 - 4gn}}{2g^2 n(r+n+1)\sqrt{(g+n+r(g+1))^2 - 4gn}}.$$

Let $A = g(n(r-1)+r(r+1)) + (r+n)^2$ and $B = (r+n)\sqrt{(g+n+r(g+1))^2 - 4gn}$. Then, $A^2 - B^2 = -4g^2 nr(r+n+1) \leq 0$ and, hence, $\frac{\partial x^*_{\text{olig}}}{\partial g} \leq 0$. Similarly, we can show that:

$$\frac{\partial x^*_{\text{olig}}}{\partial r} = \frac{-(r+n+g^2 n(r+1)+g(r+1+n(n+r+4))) + (1-gn)\sqrt{(g+n+r(g+1))^2 - 4gn}}{2gn(r+n+1)^2\sqrt{(g+n+r(g+1))^2 - 4gn}}.$$

Let $A = r+n+g^2 n(r+1)+g(r+1+n(n+r+4))$ and $B = (1-gn)\sqrt{(g+n+r(g+1))^2 - 4gn}$. Since $A^2 - B^2 = -4g(g+1)^2 n(r+n+1) \leq 0$, $\frac{\partial x^*_{\text{olig}}}{\partial r} \leq 0$. To show that $x^*_{\text{olig}}$ is a decreasing function of $n$, we note that:

$$\frac{\partial x^*_{\text{olig}}}{\partial n} = \frac{A - B}{2gn^2(r+n+1)^2\sqrt{(g+n+r(g+1))^2 - 4gn}},$$

where $A = g^2(r+1)^2(r+2n+1) + (r+n)(r+(r+n)^2 + g(3n^2(r-1) + 2r(r+1)^2 + n(r+1)(5r-1))$ and $B = (r+(r+n)^2 + g(2n^2 + 2n(r+1) + (r+1)^2))\sqrt{(g+n+r(g+1))^2 - 4gn}$. Since, $A^2 - B^2 = -4g(g+1)n^2(r+n+1)^2((g-n)^2 + r + 2(g+1)(g+n)r + (g+1)^2 r^2) \leq 0$, we conclude that $\frac{\partial x^*_{\text{olig}}}{\partial n} \leq 0$.

Let $y = 1 - nx^*_{\text{olig}} = \frac{g(r+1)-n-r+\sqrt{(g+n+r+gr)^2-4gn}}{2g(1+n+r)}$; after some algebraic manipulations, we can show that:

$$\frac{\partial y}{\partial r} = \frac{n+1-y+gny}{(r+n+1)(r+n-g(r+1)+2gy(r+n+1))}.$$

Since $\frac{\partial x^*_{\text{olig}}}{\partial g} \leq 0$, $\frac{\partial y}{\partial g} = -n\frac{\partial x^*_{\text{olig}}}{\partial g} \geq 0$.

The equilibrium price can now be expressed as $p^*_{\text{olig}} = (1+gy)y^r$. Taking partial derivative w.r.t. $g$, we get:

$$\frac{\partial p^*_{\text{olig}}}{\partial g} = \frac{p^*_{\text{olig}}}{y}\left[\left(r + \frac{gy}{1+gy}\right)\frac{\partial y}{\partial g} + \frac{y^2}{1+gy}\right] \geq 0.$$

Taking partial derivative of $p^*_{\text{olig}} = (1+gy)y^r$ w.r.t. $r$, we get:

$$\begin{aligned}\frac{\partial p^*_{\text{olig}}}{\partial r} &= \frac{p^*_{\text{olig}}}{y}\left[\left(r+\frac{gy}{1+gy}\right)\frac{\partial y}{\partial r}+y\ln(y)\right] \\ &\leq \frac{p^*_{\text{olig}}}{y}\left[\left(r+\frac{gy}{1+gy}\right)\frac{\partial y}{\partial r}-\frac{y(1-y)(11-7y+2y^2)}{6}\right], \end{aligned} \tag{A3}$$

because from power series expansion of $\ln(y)$, we can show that $\ln(y) \leq -\frac{(1-y)(11-7y+2y^2)}{6}$. We can also show that $y$ is bounded by two limits $y_1$ and $y_2$: $y_1 \leq y \leq y_2$, where

$$y_1 = \frac{g+(g+n)r+r^2}{(n+r)^2+g(1+n+r)} \text{ and } y_2 = \frac{gn(1+r)+r(1+n+r)}{n^2+r+2nr+r^2+gn(1+n+r)}.$$

Now $\left(r+\frac{gy}{1+gy}\right)\frac{\partial y}{\partial r}$ is a decreasing function of $y$, and achieves its maximum at $y=y_1$. On the other hand, $\frac{y(1-y)(11-7y+2y^2)}{6}$ is a concave function of $y$, and its minimum happens at one of the two limits, $y_1$ or $y_2$. To complete the proof, we can show, after some algebra, that:

$$\begin{aligned}\left(r+\frac{gy_1}{1+gy_1}\right)\frac{\partial y}{\partial r}\bigg|_{y_1} - \frac{y_1(1-y_1)(11-7y_1+2y_1^2)}{6} &\leq 0, \text{ and} \\ \left(r+\frac{gy_1}{1+gy_1}\right)\frac{\partial y}{\partial r}\bigg|_{y_1} - \frac{y_2(1-y_2)(11-7y_2+2y_2^2)}{6} &\leq 0.\end{aligned}$$

Finally, taking partial derivative of $p^*_{\text{olig}} = (1+gy)y^r$ w.r.t. $n$, we get:

$$\frac{\partial p^*_{\text{olig}}}{\partial n} = \frac{p}{y}\left(r+\frac{gy}{1+gy}\right)\frac{\partial y}{\partial n}.$$

Therefore, to complete the proof, we simply need to show that $\frac{\partial y}{\partial n} \leq 0$. We see that:

$$\frac{\partial y}{\partial n} = \frac{A-B}{2g(r+n+1)^2\sqrt{(g+n+r(g+1))^2-4gn}},$$

where $A = r+n-g(n(r-1)+(g+1)(r+1)^2)$ and $B = (1+g(r+1))\sqrt{(g+n+r(g+1))^2-4gn}$. Since, $A^2-B^2 = -4g(g+1)r(r+n+1)^2 \leq 0$, we conclude that $\frac{\partial y}{\partial n} \leq 0$ and $\frac{\partial p^*_{\text{olig}}}{\partial n} \leq 0$.

As before, let $y = 1-nx^*_{\text{olig}}$. The revenue can then be expressed as $R_{\text{olig}}\left(x^*_{\text{olig}}\right) = \frac{1}{n}(1+gy)(1-y)y^r$. Therefore:

$$n\frac{\partial R_{\text{olig}}\left(x^*_{\text{olig}}\right)}{\partial g} = A\frac{\partial y}{\partial g}+(1-y)y^{r+1},$$

where

$$A = \left(g(1-y)y^r + r(1-y)y^{-1+r}(1+gy) - y^r(1+gy)\right).$$

Substituting $y = \frac{g(r+1)-n-r+\sqrt{(g+n+r+gr)^2-4gn}}{2g(1+n+r)}$, we find that:

$$A = \frac{y^r(g+1)(n-1)}{2^{r-1}\left(2+g+n+r+gr-\sqrt{(g+n+r+gr)^2-4gn}\right)} \geq 0.$$

We already know that $\frac{\partial y}{\partial g} \geq 0$ (see the proof of Corollary 3). Therefore, $\frac{\partial R_{\text{olig}}\left(x^*_{\text{olig}}\right)}{\partial g} \geq 0$. Next, we know:

$$\frac{\partial R_{\text{olig}}(x^*_{\text{olig}})}{\partial r} = p^*_{\text{olig}}\frac{\partial x^*_{\text{olig}}}{\partial r}+x^*_{\text{olig}}\frac{\partial p^*_{\text{olig}}}{\partial r}.$$

Since $p^*_{\text{olig}} > 0$, $x^*_{\text{olig}} > 0$, $\frac{\partial x^*_{\text{olig}}}{\partial r} \leq 0$, and $\frac{\partial p^*_{\text{olig}}}{\partial r} \leq 0$, it is clear that $\frac{\partial R_{\text{olig}}\left(x^*_{\text{olig}}\right)}{\partial r} \leq 0$. Similarly:

$$\frac{\partial R_{\text{olig}}(x^*_{\text{olig}})}{\partial n} = p^*_{\text{olig}} \frac{\partial x^*_{\text{olig}}}{\partial n} + x^*_{\text{olig}} \frac{\partial p^*_{\text{olig}}}{\partial n}.$$

Since $p^*_{\text{olig}} > 0$, $x^*_{\text{olig}} > 0$, $\frac{\partial x^*_{\text{olig}}}{\partial n} \leq 0$, and $\frac{\partial p^*_{\text{olig}}}{\partial n} \leq 0$, it is clear that $\frac{\partial R_{\text{olig}}\left(x^*_{\text{olig}}\right)}{\partial n} \leq 0$. ■

## Proof of Theorem 4

This is straightforward from Corollary 3. The type-I effect makes the revenue larger— $\frac{\partial R_{\text{olig}}\left(x^*_{\text{olig}}\right)}{\partial g} \geq 0$ — and attracts more vendors, whereas the type-II effect reduces the revenue— $\frac{\partial R_{\text{olig}}\left(x^*_{\text{olig}}\right)}{\partial r} \leq 0$ — and makes the market less attractive to prospective vendors. ■

## Proof of Theorem 5

Straightforward from the comparison of Equations (2) and (19). ■