To disconnect or not: a cybersecurity game

By Jin Hyuk Choi, Yun-Sik Choi, Gene Moo Lee, and Andrew B. Whinston

In the cybersecurity context, we describe a continuous time game between a profit-maximizing attacker and an uninformed-defender who stops the game based on the noisy observation of action by the counterpart. The equilibrium of the game characterizes the attacker's strategy of balancing the instantaneous profit and the duration of the game. In equilibrium, the defender disconnects the counterpart when the updated suspicion level is above certain threshold. Our analysis implies that strategic defense of the Internet Service Providers (ISPs) is necessary for the viability of the Internet-based society. We provide sufficient conditions of the model parameters to attract ISPs to play the role of the defender.

I. Introduction

Our daily lives, business operations, and government services heavily rely on the Internet infrastructure. As our dependency on cyberspace has increased, however, so has the number of cyber threats and associated financial damages, rendering cybersecurity a critical societal issue.[1] Well-organized hackers operate as for-profit businesses seeking to maximize profit, where the profit can be based on the cumulative attack-intensity.[2] The defending side, such as cybersecurity service providers, and governments, is also taking active measures to cope with cyberattacks. Governments are implementing new cyber policies,[3] while using intelligence to track down high-profile cyber attackers.[4] Cybersecurity service providers analyze new threats every day and develop both hardware and software solutions for their clients. Even with the technological advances in the security systems and the policy implementations, cyber risk will continue to exist due to the strategic actions by the financially motivated attackers – cyber risk is a factor that has to be managed rather eliminated.

We introduce a game model to study interaction between attacker and defender in the cybersecurity framework, and discuss how perception of defender affects the viability of Internet-based society. In the game, we naturally consider Internet Service Providers (ISPs) as the defender, since ISPs can monitor network traffics and use Traffic Analysis to detect anomalies in traffic patterns (see (Chen

[1] See Annual Internet security threat report (2016) by Symantec Corporation.

[2] For example, the attack-intensity can be volume of spam emails, or intensity of distributed denial-of-service (DDoS) attacks.

[3] See https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-orderimproving-critical-infrastructure-cybersecurity.

[4] (He et al. 2016) conduct randomized field experiment and provide a causal evidence that proper policy implementation can significantly mitigate cyberattacks.

and Lin 2015)). As a defender, ISP can proactively disconnect suspicious entities and reduce expected damages by cyberattacks. To reflect the aforementioned characteristics of cybersecurity, we develop a continuous time game model with ingredients of defender's optimal stopping and attacker's long-lived private information. To the best of our knowledge, our model is the first game model including these ingredients.

Specifically, the game starts when a user, potentially an attacker, initiates a connection with the defender. The user can be either an attacker[5] or an innocent user, which the defender does not know a priori. The defender dynamically updates the probability (suspicion level) of the user being an attacker. Based on the suspicion level, defender optimally chooses when to block (disconnect) the user to minimize the expected cost – sum of the costs by attacker and false alarm costs. In case the user is an attacker, it dynamically chooses the attack-intensity to maximize the expected profit that can be obtained until it is blocked by the defender. Then, the strategic interaction between the players leads to a Bayesian Nash equilibrium, which consists of the attacker's optimal strategy and the defender's optimal disconnection policy.

We find the unique explicit Bayesian Nash equilibrium, and provide verification for the optimization problems of the attacker and defender. The explicit form of the equilibrium enables us to interpret the behaviors of the players. As the suspicion level getting closer to the block threshold, the attack-intensity decreases and the defender becomes less sensitive to the signal process. In other words, both attacker and defender are less active when the suspicion level is about to cross the redline. The equilibrium block threshold decreases (the defender blocks the users more occasionally) if (i) the upper bound of attack-intensity increases, (ii) the signal process is more noisy (less informative), (iii) the false alarm cost of the defender decreases, and (iv) the chance of random detection of the attacker decreases (e.g., antivirus software improvement become slow).

Our analysis leads to insights on viability of Internet-based society. Rapid expansion of network-enabled devices and faster Internet speed provide more attack possibilities (i.e., higher upper bound of attack-intensity in the game). Will the cost due to cyberattack explode as the upper bound of attack-intensity getting higher? To answer this question, we compare our baseline equilibrium result with three benchmark cases. We show that the expected cost converges to a finite number, if the defender takes into account the strategic nature of the attacker when updating the suspicion level. Otherwise, the expected cost explodes as the upper bound of attack-intensity gets higher. We conclude that the defender's roles of updating suspicion level and blocking suspicious users are essential for the viability of the Internet-based society.

The baseline model implies that ISPs are in the suitable position to provide managed security service with warranty (MSSW), in addition to traditional Internet access services. To reduce cyber risk and related costs, ISPs can play the

[5]For example, the user can be a PC with malware, controlled by a bot master.

role of the defender in our game model – blocking suspicious entities based on the historical traffic information. We provide a formula that can be used for the calibration of the initial suspicion level, which is a core model parameter. Playing the game multiple times, ISPs can calibrate the model parameters more effectively than individual hosts. On the other hand, in reality, the market for MSSW is still underdeveloped and only a few ISPs provide managed security service. To explain this phenomenon, we extend our baseline model to include the *monitoring cost*. The analysis of the extended model shows that the MSSW business is profitable if (i) the upper bound of attack-intensity is high enough, (ii) the monitoring cost is low enough, or (iii) the chance of random detection of the attacker is small enough. We expect that MSSW business to thrive in near future, because the Internet security situation tends toward aforementioned three conditions.

The distinctive feature of our model is to endogenize defender's blocking policy of when to terminate the game. Many of economic decisions can be seen as a problem of when to quit (or start) certain relationship with the other economic entity whose type is a private information. Beyond the cybersecurity case, our game framework is general enough to be applicable for setting policies like following examples: guideline for police officers when to arrest a suspect based on abnormal behaviors of the suspect, United Nations' policy for when to initiate sanctions against possibly dangerous countries, German's decision in World War II whether to renounce Enigma (an encryption system) or not considering the possibility that Allies already have decryption method for Enigma, a company's human resource criteria for dismissing employees based on their behaviors.

Our model is related to insider trading literature in finance. (Kyle 1985) describes interaction of market makers and an insider who has long-lived private information about an asset value, and studies equilibrium pricing of the market makers and dynamic trading of the insider. A version of Kyle model studied in (Back and Baruch 2004) is close to our model: their insider has private information of binary asset value and our suspect has private information about her identity which is binary (attacker or innocent user); their market makers update price of the asset and our defender updates suspicion level.

Attacker in our model strategically control her action to hide her identity from defender, and this ingredient of model is connected to deception literature in game theory. (Hendricks and McAfee 2006) consider a one-shot game with sender and receiver, and describes how the signaling technology affects equilibrium strategy of the attacker. (Crawford 2003) shows that in the interaction of rational and boundedly rational types of players, the deception can be used by rational type. (Aumann and Maschler 1966) study dynamic game of incomplete information in discrete time framework.

The closest model to ours is the model in (Anderson and Smith 2013). Private information and profit structure of attacker in our model is similar to those of the attacker in (Anderson and Smith 2013). Accordingly, the equilibrium attacking intensities are analogous. But the role of defender in our model is qualitatively

different from theirs. (Anderson and Smith 2013) consider continuum of myopic defenders who instantaneously choose mixed strategy of binary actions. On contrast, we consider a single defender who terminates the game to minimize the cumulative expected cost.

Our model can be also considered as a game version of the sequential testing literature in mathematics statistics.[6] Based on the continuous observation of user's actions, the defender's task is to test sequentially the hypothesis whether the user is the attacker or not, and to find the optimal stopping policy to minimize the expected cost. In other words, the defender side narrative in our model is to solve a sequential testing problem for hypothesis about the drift part of an observed Gaussian process. The key difference between our game model and the sequential testing problem is that our defender is dealing with the strategic attacker who takes into account the defenders strategy – the sequential test results are provided by an adversarial counterpart.

II. The Model

We consider a continuous time game between a user (who can be either an attacker or an innocent user) and a defender. The identity of the user is represented by a random variable θ which can take two values 0 or 1: $\theta = 1$ means that the user is an attacker and $\theta = 0$ means that the user is an innocent user. The defender is uninformed about the value of θ, and has prior $q_0 = \mathbb{E}[\theta] \in (0, 1)$ which is the defender's initial estimation of probability that the user is an attacker. In case the user is an innocent one, the user performs no malicious action. Otherwise, the attacker chooses the attack-intensity Δ_t dynamically over time $t \geq 0$. We set a constant $M > 0$ as the upper bound for attack-intensity, i.e., $0 \leq \Delta_t \leq M$ for all $t \geq 0$.

We consider the defender who can disconnect the user and terminate the game, based on the observation of the user's action. We assume that the defender's observation of the user's action flow $\Delta_t 1_{\{\theta=1\}} dt$ is obscured by a noise term $\sigma\, dW_t$, where $\sigma > 0$ is a constant and $(W_t)_{t\in[0,\infty)}$ is a standard Brownian motion independent of θ.[7] In other words, the signal process $(Y_t)_{t\in[0,\infty)}$ the defender can observe is expressed as:

$$dY_t = \Delta_t 1_{\{\theta=1\}} dt + \sigma\, dW_t. \tag{II.1}$$

Based on the available information up to time t obtained by the observation of the signal process Y, the defender can updated the suspicion level q_t (the defender's

[6] The history of the sequential testing problems is long and we only mention (Wald 1945) and (Wald and Wolfowitz 1949) here.

[7] One way to interpret this is to consider $\Delta_t dt$ as the malicious action by generated by the bot master and $\sigma\, dW_t$ as the normal traffic by the original owner of the computer.

estimation of probability that the user is an attacker), i.e.,

$$q_t = \mathbb{P}(\theta = 1 | \mathcal{F}_t^Y), \tag{II.2}$$

where $(\mathcal{F}_t^Y)_{t\in[0,\infty)}$ is the filtration generated by the process Y. We assume that the signal process Y is public information and known to the attacker. This implies the admissibility condition $\Delta_t \in \mathcal{F}_t^Y$ for the attacker strategy. The filtering equation (II.2) produces[8] the following Stochastic Differential Equation (SDE) that q_t should satisfiy:[9]

$$\begin{aligned} dq_t &= \frac{1}{\sigma^2}\Big(\mathbb{E}[\theta\,\Delta_t 1_{\{\theta=1\}}|\mathcal{F}_t^Y] - \mathbb{E}[\theta|\mathcal{F}_t^Y]\cdot\mathbb{E}[\Delta_t 1_{\{\theta=1\}}|\mathcal{F}_t^Y]\Big) \\ &\qquad \cdot \Big(dY_t - \mathbb{E}[\Delta_t 1_{\{\theta=1\}}|\mathcal{F}_t^Y]dt\Big) \\ &= \frac{q_t(1-q_t)\Delta_t}{\sigma^2}\Big(dY_t - q_t\Delta_t dt\Big) \end{aligned} \tag{II.3}$$

We consider a game between the attacker and defender, and the Bayesian Nash equilibrium consists of (i) the attacker's optimal strategy and (ii) the defender's optimal stopping strategy.

(i) Attacker's profit maximization problem

The attacker obtains instantaneous profit of $\Delta_t dt$ through her malicious actions. The game is over when the identity of the user is randomly revealed (at time T) or the defender disconnects the user (at time τ_p). We assume that T is independent of θ and $(W_t)_{t\in[0,\infty)}$, and has exponential distribution,

$$\mathbb{P}(T > t) = e^{-rt}, \tag{II.4}$$

with a constant $r > 0$. The stopping time τ_p is defined as[10]

$$\tau_p = \inf\{t \geq 0 : q_t \geq p\}, \tag{II.5}$$

i.e., the defender disconnect the user when the suspicion level q_t is above certain threshold $p \in (0, 1)$.

The attacker seeks the optimal strategy Δ to maximize her expected cumulative profit until the game is over:

$$\max_{0\leq(\Delta_t)_{t\in[0,\infty)}\leq M} \mathbb{E}\Big[\int_0^{T\wedge\tau_p} \Delta_t dt \,\Big|\, \theta = 1\Big]. \tag{II.6}$$

[8] See (Liptser and Shiryaev 2001) Theorem 8.1.

[9] In (II.3), the term $dY_t - q_t\Delta_t dt$ is innovation (or surprise) the defender perceives. (II.3) says that the adjustment of q is proportional to the surprise. The term $q_t(1-q_t)\Delta_t/\sigma^2$ describes how sensitively the belief changes with respect to the surprise.

[10] τ_p is a stopping time respect to the filtration $(\mathcal{F}_t^Y)_{t\in[0,\infty)}$.

The attacker recognizes that her actions affect the stopping time τ_p in such a way that more aggressive actions (larger Δ) will increase the suspicion level q faster through the defender's Bayesian update, and eventually terminate the game sooner (smaller τ_p).

(ii) Defender's cost minimization problem

We assume that the defender has two types of costs - cumulative cost from malicious actions of attacker in case $\theta = 1$, and one-time cost of *false alarm* if the defender disconnects an innocent user. To describe the class of admissible strategies of the defender, let $\mathcal{T}$ be the set of all stopping times with respect to the filtration $(\mathcal{F}_t^Y)_{t\in[0,\infty)}$. The defender's goal is to find the optimal disconnecting strategy to minimize the expected total costs:

$$\min_{\tau\in\mathcal{T}} \mathbb{E}\Big[\Big(\int_0^{T\wedge\tau} \Delta_t dt\Big)\cdot 1_{\{\theta=1\}} + l_f \cdot 1_{\{\theta=0,\,\tau<T\}}\Big], \tag{II.7}$$

where the constant $l_f > 0$ is the one-time-cost of blocking an innocent user. We can check that two extreme cases produce trivial optimal stopping strategy: In case $l_f = 0$, then the defender should block the user immediately, i.e., set $\tau \equiv 0$; If $l_f = \infty$, then the defender never block the user, i.e., set $\tau \equiv \infty$.

The optimal stopping strategy τ is endogenously determined by the defender's optimization problem. This feature of termination of game based on the suspicion level is the distinctive ingredient of our model compared to existing Bayesian game models: (Kyle 1985) considers fixed terminal time; (Back and Baruch 2004) and (Anderson and Smith 2013) set the terminal time as an independent random time, as T in this paper, which is not part of equilibria.

In this framework, our goal is to study Bayesian Nash equilibrium that consists of the attacker's optimal strategy and the defender's optimal stopping strategy. The definition of the equilibrium is following.

DEFINITION II.1: *Consider a constant $p \in (0,1)$ and a Lipschitz continuous function $\alpha : [0,1] \to [0,M]$. Let $(Y_t)_{t\geq 0}$ be as in* (II.1) *and τ_p as in* (II.5)*. We say that the pair (p,α) is a Bayesian Nash equilibrium if following (1) and (2) hold.*

(1) (Attacker's optimal intensity) Let $(q_t)_{t\geq 0}$ obeys the SDE[11]

$$dq_t = \frac{q_t(1-q_t)\alpha(q_t)}{\sigma^2}\Big(dY_t - q_t\alpha(q_t)dt\Big). \tag{II.8}$$

Then, $\big(\alpha(q_t)\big)_{t\geq 0}$ is the solution of the attacker's profit maximization problem, i.e.,

$$\big(\alpha(q_t)\big)_{t\geq 0} \in \underset{0\leq(\Delta_t)_{t\in[0,\infty)}\leq M}{\arg\max}\ \mathbb{E}\Big[\int_0^{T\wedge\tau_p} \Delta_t dt \,\Big|\, \theta = 1\Big]. \tag{II.9}$$

[11] This SDE is originated from the update of belief, (II.2), and its SDE form (II.3).

(2) (Defender's optimal stopping) Let $(q_t)_{t\geq 0}$ *obeys the SDE* (II.8) *with* $\Delta_t = \alpha(q_t)$*. Then, the stopping time* τ_p *solves the defender's cost minimization problem:*

$$\tau_p \in \arg\min_{\tau\in\mathcal{T}} \mathbb{E}\Big[\Big(\int_0^{T\wedge\tau} \alpha(q_t)dt\Big)\cdot 1_{\{\theta=1\}} + l_f \cdot 1_{\{\theta=0,\,\tau<T\}}\Big], \tag{II.10}$$

where $\mathcal{T}$ *be the set of all stopping times with respect to the filtration* $(\mathcal{F}_t^Y)_{t\geq 0}$*.*

To clarify, the exogenously given model parameters are q_0, r, M, σ and l_f, and the endogenously determined quantities through our Markovian equilibrium are attacker's optimal strategy α and defender's optimal stopping policy p.

THEOREM II.2: *There exists a Bayesian Nash equilibrium* (p, α)*.*

The proof of Theorem II.2 and the explicit formula of the equilibrium (see Proposition VII.2) are given in Appendix.

REMARK II.3: *(Uniqueness of the equilibrium) From Definition II.1, we derive the system (*(VII.6), (VII.7) *and* (VII.11)-(VII.13)*) of differential equations and inequalities in Appendix. The Bayesian Nash equilibrium in* (II.2) *is unique in the sense that the system (*(VII.6), (VII.7) *and* (VII.11)-(VII.13)*) has a unique solution.*

As a real-world example, we can apply our model to the botnet and botherder situation. Botherders[12] never attack targets with their own machines, and use their botnet as a front line army. Each botnet consists of many individual bots which are compromised Internet connected devices such as personal computers, tablets, or Internet-of-Things (IoT) devices. In most cases, the owners of compromised devices will use their machines daily without being aware of the existence of bots. This regular activity is modeled as noise dW_t in (II.1), and the malicious activity of a bot is denoted by $\Delta_t dt$. The defender updates the suspicion level q_t based on the signal Y_t, which is sum of the regular activity of the owner of the device and the malicious activity generated by the bot. In addition, most ordinary users do not try to hide themselves or jump around different Internet Protocol (IP) addresses for their privacy. In our model, the goal of the defender is not eliminating botherders which is very complicate and difficult task, but blocking the compromised hosts who are directly affecting the customers. Depending on the type of the botherders, some bots remain silently and attack strategically under noise,[13] and some others attack untactfully and get detected earlier. We consider several different situations regarding the type of the attacker in Section III.

[12] A malicious hacker who controls a botnet (many bot-infected devices) to attack targets.

[13] See Jaku botnet example: https://www.helpnetsecurity.com/2016/05/05/jaku-botnet-targeted-attacks/

III. Viability of the Internet-based society

Expansion of the Internet capacity due to the increase of network-enabled devices and faster Internet speed introduced more cybersecurity related issues.[14] For cyber attackers, more Internet capacity implies more attack capacity, that is, higher M in our model.

In this section, we extract our model's implication regarding this issue of increasing attack capacity. We analyze the relationship between M (the maximum attack-intensity) and the equilibrium costs of the defender. In addition to our original game model, we consider three benchmark cases below, as stepping stones to the path to our equilibrium. We explain motives of the attacker or defender to be more *strategic*: each case should naturally evolve to the next case, and finally we reach the case of our baseline equilibrium.

A. Case of no-defence

To begin with, we consider the case the defender does nothing. Then there is no reason for attacker to hide its identity, and the attacker will choose attack-intensity as M all the time. The corresponding expected profit $V_1(q_0)$ of the attacker and expected cost $C_1(q_0)$ of the defender are easily computed:

$$\begin{aligned} V_1(q_0) &= \mathbb{E}\Big[\int_0^T M\,dt \;\Big|\; \theta = 1\Big] = \frac{M}{r}, \\ C_1(q_0) &= \mathbb{E}\Big[\Big(\int_0^T M\,dt\Big)\cdot 1_{\{\theta=1\}}\Big] = \frac{q_0 M}{r}. \end{aligned} \tag{III.1}$$

We observe that $C_1(q_0) \to \infty$ as $M \to \infty$. This means that if there is no defense mechanism at all, then the Internet-based society may not be viable when the maximum attack-intensity is very high.

B. Case of non-strategic attacker vs. defender

The previous case is obviously not a desired situation for the defender side. Therefore, it is natural to expect that the defender does some defense activities: she may block the user to minimize the expected cost. In this subsection, we consider the case the attacker is not strategic, i.e., the attacker is not aware of the role of the defender and just chooses the attack-intensity as M all the time.

PROPOSITION III.1: *In the case of non-strategic attacker vs. defender (see Proposition VII.4 for detailed explanation), the optimal block threshold $\tilde{p}$, the*

[14] For example, a distributed denial of service (DDoS) attack from tens of millions of IoT devices caused several hours of blackout on domain name system (DNS) servers operated by Dyn. It was the biggest DDoS attack with an estimated throughput of 1.2 terrabits per second. Also, the Internet Protocol version 6 (IPv6) enables a lot more devices to be connected to Internet space. See https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet, and http://iot6.eu/ipv6_advantagess_for_iot.

minimal expected cost of the defender $C_2(q_0)$, and the corresponding expected profit of the attacker $V_2(q_0)$ have following asymptotic behavior:

$$\lim_{M\to\infty} \tilde{p} = 1, \quad \lim_{M\to\infty} C_2(q_0) = 0, \quad \lim_{M\to\infty} V_2(q_0) = 0. \tag{III.2}$$

Proposition III.1 says that as $M \to \infty$, the expected cost of the defender becomes negligible. Here is an intuitive explanation. When $\Delta_t = M$, the adjustment equation (II.3) becomes

$$dq_t = \frac{q_t(1-q_t)M}{\sigma^2}\Big(dY_t - q_t M dt\Big). \tag{III.3}$$

We observe that for bigger M, the the belief process q_t reacts to the surprise $(dY_t - q_t M dt)$ more sensitively, i.e., q_t moves toward the true state of θ (identity of the user) more quickly. This means that it is easier for the defender to detect the existence of the attacker, so the lifetime of the attacker decreases and the expected cost diminishes accordingly. This also implies the convergence of the block threshold $\tilde{p}$ to 1. In summary, if the attacker is non-strategic and the defender disconnects the user optimally, then the increase of M eventually harms the attacker's profit and makes attacker to be more *detectible* to the defender.

C. Case of strategic attacker vs. naïve defender

In the previous case, the non-strategic attacker will realize that its expected profit vanishes as M increases. Then it will naturally consider the defender's blocking strategy and choose attack-intensity strategically to avoid disconnection. Therefore, we now assume that the attacker is strategic, but the defender does not realize that the attacker is strategic. Still, the defender updates the suspicion level, but the adjustment equation (II.3) is driven by the assumption that the attack-intensity is always M. To be specific, we assume that $(q_t)_{t\in[0,\infty)}$ is the solution of the following SDE,

$$dq_t = \frac{q_t(1-q_t)M}{\sigma^2}\Big(dY_t - q_t M dt\Big) \quad \text{with} \quad dY_t = \Delta_t 1_{\{\theta=1\}} dt + \sigma\, dW_t, \tag{III.4}$$

where $(\Delta_t)_{t\in[0,\infty)}$ is the attackers possible strategy.[15]

PROPOSITION III.2: *In case of strategic attacker vs. naïve defender*[16] *(see Proposition VII.5 for detailed explanation), the maximum expected profit of attacker $V_3(q_0)$, and the expected cost of defender $C_3(q_0)$ have following asymptotic*

[15] Then, (III.4) will not produce the filtering equation (II.2) if the attack-intensity Δ_t is different from M.

[16] This defender is *naïve* in the sense that she believes that the attacker is non-strategic and always chooses $\Delta_t = M$.

behavior:

$$\lim_{M\to\infty} V_3(q_0) = \infty, \quad \lim_{M\to\infty} C_3(q_0) = \infty. \tag{III.5}$$

Proposition III.2 says that as $M \to \infty$, the expected cost of the defender also goes to ∞. Here is an intuitive explanation. Similarly as in the previous case, for bigger M, q_t moves toward the true state of θ more quickly. Now the 'strategic' attacker makes the situation quite different from the previous case. Proposition VII.5 in Appendix D provides the form of the optimal attack-intensity $\tilde{\alpha}$: Recall that $\tilde{p}$ is the optimal block threshold in Proposition III.1, and the constant a is defined in (VII.14). For large enough M, we have

$$\tilde{\alpha}(q_t) = \begin{cases} M, & \text{if } \ q_t \in [0, \tilde{q}^*] \\ 0, & \text{if } \ q_t \in (\tilde{q}^*, 1] \end{cases} \quad \text{where} \quad \tilde{q}^* = \frac{1}{1+(\frac{1+a}{2a^2})^{\frac{1}{1+2a}}(\frac{1-\tilde{p}}{\tilde{p}})}. \tag{III.6}$$

In words, the attacker chooses not to attack at all when the suspicion level q_t is relatively high ($q_t > \tilde{q}^*$), then the suspicion level will quickly drop with high probability. The attacker resumes the malicious activity when q_t is small enough ($q_t \leq \tilde{q}^*$). By exploiting defender's naïveness, the strategic attacker can make expected profit ∞ as $M \to \infty$.

D. Case of strategic attacker vs. defender (the baseline model in Definition II.1)

In the previous case, the naïve defender's expected cost blows up as $M \to \infty$. Therefore, the naïve defender will naturally perceive the strategic behavior of the attacker and incorporates it to the adjustment of the belief process $(q_t)_{t\in[0,\infty)}$. This is the baseline equilibrium concept in Definition II.1.

PROPOSITION III.3: *The equilibrium in Definition II.1 produces following asymptotic result for the expected cost of the defender $C_e(q_0)$ and the optimal block threshold p:*

$$\begin{aligned} \lim_{M\to\infty} C_e(q_0) &= \begin{cases} l_f(1-q_0)e^{-\varphi(1-\frac{\sigma q_0}{l_f\sqrt{\pi r}(1-q_0)})}, & q_0 \in [0,p) \\ l_f(1-q_0), & q_0 \in [p,1] \end{cases} \\ \lim_{M\to\infty} p &= \frac{l_f\sqrt{\pi r}}{l_f\sqrt{\pi r}+\sigma} \end{aligned} \tag{III.7}$$

Comparing the optimal attack strategies in the cases of Proposition III.2 and Proposition III.3, we observe that the attacker becomes more careful in Proposition III.3 and *smooths out* its extreme behavior. Figure 1 illustrates the situation. The value of $\tilde{\alpha}$ in (III.6) is M or 0 only, and it is discontinuous in q_t. On the other hand, the optimal attack strategy α in Proposition III.3 is continuous in q_t:[17] the

[17]See Theorem VII.3 for the expression of α.

attacker cannot exploit the naïveness of the defender anymore, so it gradually decreases the attack-intensity as the suspicion level increases.

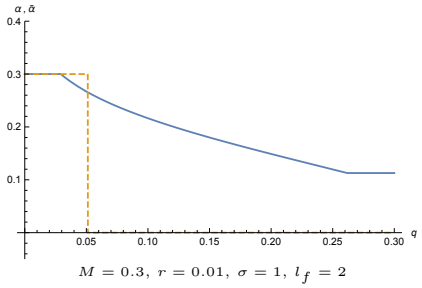


FIGURE 1. α (—) AND $\tilde{\alpha}$ (- - -)

In our equilibrium model (Definition II.1) with strategic attacker and strategic defender, Proposition III.3 implies that the expected cost and the optimal threshold stabilize as $M \to \infty$. Figure III.D illustrates that the relationships

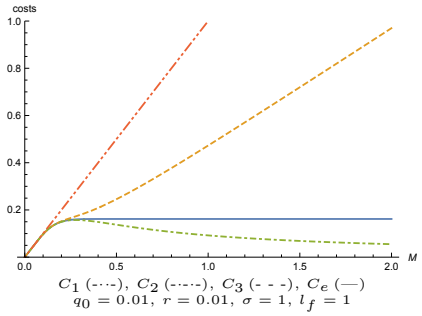


FIGURE 2. EXPECTED COSTS FOR DIFFERENT CASES, AS FUNCTIONS OF M

between M and the defender's expected costs for different cases, C_1, C_2, C_3 and C_e. From the aforementioned four cases, we derive the model implication for the requirements regarding the viability of the Internet-based society when the maximum attack capacity M is very high: (i) the defender's roles of updating suspicion level and blocking suspicious users are necessary, and (ii) the defender's updating procedure should rely on the right perception of attacker (non-strategic or strategic).[18]

[18]We may think $C_e - C_3$ as the defender's cost for the *underestimation* of the attacker, which goes to ∞ as $M \to \infty$.

IV. Equilibrium analysis

In this section we examine the equilibrium behaviors of the attacker and defender in our game. As in (Anderson and Smith 2013), the quantity $\frac{r\sigma^2}{M^2}$ plays an important role for the description of the equilibrium.

A. Block threshold

In the equilibrium of our continuous time Bayesian game model, the most distinctive feature – compared to existing literature on insider trading and deception – is that the defender terminates the game if the updated suspicion level is above certain threshold p, and the threshold is endogenously determined by the defender's cost-minimization problem. Theorem VII.3 in Appendix C shows that the equilibrium threshold p has the following form:

$$p = \begin{cases} \frac{(1+a)rl_f}{(1+a)rl_f+aM}, & \text{if } \frac{r\sigma^2}{M^2} > 1 \\ \frac{c\,l_f\sqrt{\pi r}}{c\,l_f\sqrt{\pi r}+\sigma}, & \text{if } \frac{r\sigma^2}{M^2} \leq 1 \end{cases} \tag{IV.1}$$

where a, b, c are constants (depending on r, σ, M) defined in (VII.14). For comparison, we also consider $\tilde{p} = \frac{(1+a)r\,l_f}{(1+a)r\,l_f+aM}$ in Proposition III.1, the optimal block threshold in case the defender deals with a non-strategic attacker.

PROPOSITION IV.1: *(1) $p \leq \tilde{p}$.*
(2) p decreases in M and σ, and increases in l_f and r.

Figure IV.A illustrates Proposition IV.1. The intuition for Proposition IV.1 (1) is obvious: The defender will be more careful and lower the block threshold when she encounters the strategic attacker, rather than non-strategic one. The intuition for Proposition IV.1 (2) is following: (i) Larger σ makes the observation $(Y_t)_{t\geq 0}$ more noisy and less informative for the defender. Accordingly, the attacker will be more aggressive since its identity is harder to be detected, and the expected cost of the defender will increase. Therefore, for larger σ, the defender will be more cautious and lower the block threshold. (ii) Larger l_f (the false alarm cost) makes the defender more reluctant to block the user, therefore, induces higher equilibrium block threshold. (iii) Recall that T represents the random time when the identity of the user is revealed, and it is assumed to have the exponential distribution (II.4). If we increase r, then the defender has a better chance of finishing the game without concern of the false alarm cost. Therefore, larger r makes the defender to rely more on the random termination of game, and increases the equilibrium block threshold. (iv) The M-dependence is more subtle than the others. We consider non-strategic attacker case first. If M increases, than the non-strategic attacker's instantaneous profit increases (downward effect for $\tilde{p}$) but the defender updates the suspicion level more sensitively on the signal (see (III.3)), i.e., the attacker's identity is more revealing (upward effect for $\tilde{p}$).

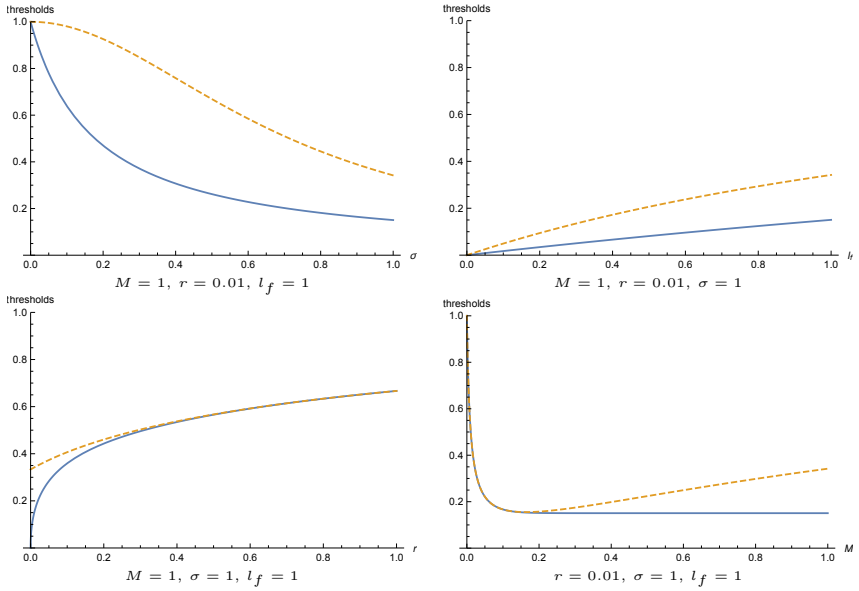


FIGURE 3. p (—) AND $\tilde{p}$ (- - -) FOR VARYING l, r, σ, AND M

These upward and downward effects on $\tilde{p}$ can be seen in Figure IV.A for varying M, first decreasing then increasing. When M is large enough, the existence of the non-strategic attacker is very revealing. In contrast to $\tilde{p}$, p is monotonically decreasing on M. We deduce that for large enough M, the strategic attacker refrains itself from aggressive actions and mitigates the revealing effect. This observation is consistent with the attacker's behavior in equilibrium (see (2) in Proposition IV.2).

Observe that the gap between p and $\tilde{p}$ increases in M. This implies that when the maximum attack capacity is high, it is important for the defender to notice that the attacker is strategic. Otherwise, if the defender naïvely assumes that the attacker is non-strategic, then he will choose block threshold much higher than p (the truly optimal one) and will suffer higher expected cost (see Figure III.D).

B. Attacker's strategy

The attacker dynamically optimizes the attack-intensity to maximize the expected profit, under the consideration that the defender updates the suspicion level by the signal process. The explicit expression of the equilibrium in Theorem VII.2 implies the following property of the optimal strategy of the attacker.

PROPOSITION IV.2: *(1) If* $\frac{r\sigma^2}{M^2} \geq 1$*, the attacker chooses maximum attack-intensity, i.e,* $\alpha = M$*, all the time regardless of the suspicion level.*

(2) If $\frac{r\sigma^2}{M^2} < 1$*, the attacker chooses maximum attack-intensity* M *when* $q_t \leq q^*$*. After* q_t *exceed* q^**, the attack-intensity gradually decreases as* q_t *increases. The*

expression of q^* *is in* (VII.14).

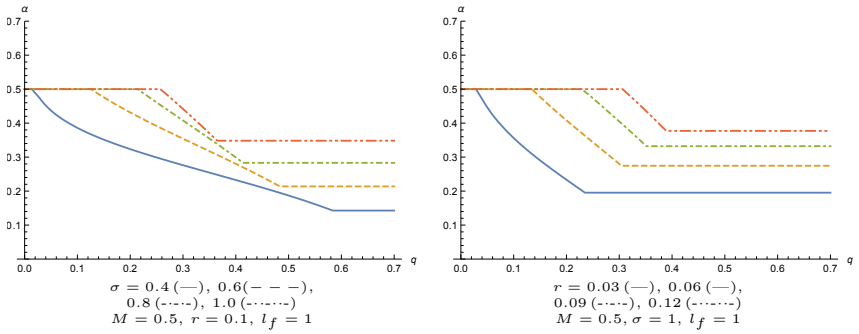


FIGURE 4. GRAPHS OF $\alpha(q)$

Figure 4 describes Proposition IV.2. This behavior of the attacker is similar to that of (Anderson and Smith 2013), in the sense that the attacker is *deceptive*: When the suspicion level q_t is high, the attacker reduces attack-intensity to mitigate the increase of q_t. The key difference between our model and one in (Anderson and Smith 2013) is that our defender terminates the game when q_t reaches the block threshold p, therefore, our attacker's behavior can be interpreted as sacrificing the current profit to extend the lifetime of the game.

Figure 4 also shows that the attack-intensity increases as σ or r increases: (i) If there is more noise (larger σ), then it is easier for the attacker to hide its identity, so the attack-intensity will be higher. (ii) If we increase r, then there is more chance for the random termination of game, which makes the attacker's *deception* less valuable. Therefore, the attacker will focus more on the current profit (less on the lifetime of the game) and be aggressive as r increases.

C. Defender's adjustment of suspicion level

The defender updates q_t by (II.8) in equilibrium, and q_t becomes the belief of the defender that the user is an attacker, i.e, q_t satisfies (II.2). From the form of the adjustment equation (II.8), we define a function λ as follows:

$$\lambda(q_t) := \frac{q_t(1-q_t)\alpha(q_t)}{\sigma^2}. \tag{IV.2}$$

Then λ represents the sensitivity of the movement of q_t with respect to the signal process dY_t.[19]

The following proposition implies that the update of the suspicion level q_t becomes less sensitive to the signal dY_t when q_t is close to the block threshold, or the false alarm cost l_f decreases.

[19]This λ corresponds to price impact function (Kyle's lambda) in the insider trading literature.

PROPOSITION IV.3: *(1) If* $\frac{r\sigma^2}{M^2} < 1$, *then* $\lim_{q\uparrow p} \lambda'(q) < 0$.
(2) λ *is increasing in* l_f.

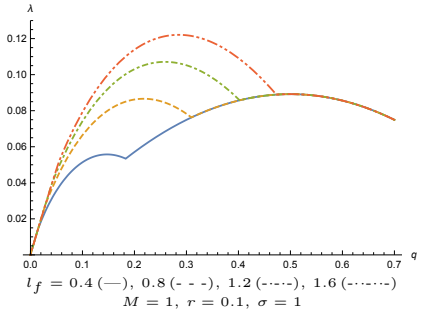


FIGURE 5. GRAPHS OF $\lambda(q)$

Figure 5 illustrates Proposition IV.3. Proposition IV.3 (1) indicates that λ decreases on q near p. Here is an economic intuition. If $\frac{r\sigma^2}{M^2} < 1$, then Proposition IV.2 implies that the attacker will be less aggressive when q_t is close to p. In other words, the attacker's portion α becomes relatively small in the signal dY_t. This implies that the signal becomes less informative for the defender, so the defender will reduce the sensitivity λ. Therefore, when the suspicion level is close to the block threshold, both attacker and defender become *less active*.

We also give an intuitive explanation for (2) in Proposition IV.3. According to Proposition IV.1, p is increasing in l_f, hence it is enough to explain why $\lambda(q_t)$ increases in p. For higher block threshold p, the attacker will be more aggressive since it is harder to be blocked. Then the signal Y_t will be more informative for the defender, so λ will be bigger.

V. Business model for ISPs - MSSW provider

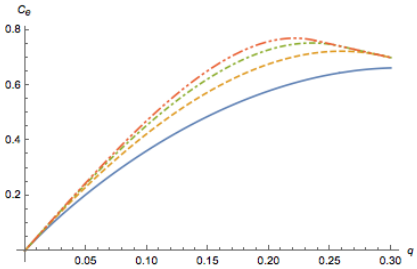
We suggest ISPs to provide MSSW for the clients who cannot afford a state of the art, in-house security system and cybersecurity experts. In this way, the liability of ISPs becomes a financial motive for strategic defense, as in our game model. The ISP will engage in more efficient defense to reduce the costs, and the expected societal costs related to cyberattacks will decrease accordingly. This produces a win-win situation for the clients, ISPs, and society.

Our game model supports the claim that ISPs are in the suitable position to take the role of defender. The defender reduces the expected cost by strategically blocking the user based on the observation of the signal process. The "observe & update" role of the defender can be more effectively performed by ISPs than individual hosts, because ISPs have collective knowledge of the state of the Internet. For instance, the defender need to assign the initial suspicion level q_0. The following proposition can be used for the estimation of q_0.

PROPOSITION V.1: *For $0 < q_0 < p$, the probability that the defender eventually blocks a user is given by*

$$\mathbb{P}(\tau_p < \infty) = \frac{q_0}{p}. \tag{V.1}$$

According to (V.1), $q_0 \approx p \cdot$ (ratio of blocked users). To make this calibration more accurate, the defender is supposed to be in the position to play multiple games with different users. Naturally, ISPs are in the optimal position for such tasks since dealing with multiple entities is their original job.



$\sigma = 1.0\,(—),\ 1.5(- - -),\ 2.0\,(\text{-·-·-}),\ 2.5\,(\text{-··-··-}),$
$M = 0.5,\ r = 0.1,\ l = 1$

FIGURE 6. GRAPHS OF $C_e(q)$

In Figure 6, we observe that the expected cost of the defender increase over the noise term σ. This means that ISP with better filtering ability (small σ) can reduce the MSSW fee and attract more customers.

Even though some ISPs including AT&T and Verizon are providing managed security service, the market for the service is very limited and underdeveloped. To explain this situation, we extend our game model to include *monitoring cost*. To be specific, we modify the defender's cost minimization problem (II.10) in Definition II.1 the following:

$$\tau_p \in \arg\min_{\tau \in \mathcal{T}} \mathbb{E}\Big[\Big(\int_0^{T\wedge\tau} \alpha(q_t)dt\Big) \cdot 1_{\{\theta=1\}} + \int_0^{T\wedge\tau} l_s\, dt + l_f \cdot 1_{\{\theta=0,\, \tau<T\}}\Big], \tag{V.2}$$

where the constant $l_s \geq 0$ represents the monitoring cost.[20] If the monitoring cost l_s is too high, then it is better not provide such service.

We show in Theorem VII.7 that there exists an equilibrium if $l_s < r\ l_f$. The following result implies explanation for the premature state of the MSSW market.

[20] Traffic stream analysis requires some costs.

PROPOSITION V.2: *Assume that $l_s < r\ l_f$. Then there exists an equilibrium in Definition II.1 with the defender's cost minimization problem* (V.2). *The defender's equilibrium expected cost is less than $C_1(q_0) = \frac{q_0 M}{r}$ (the cost without defense) if (i) M is large enough, (ii) r is small enough, or (iii) l_s is small enough.*

Proposition V.2 indicates that the MSSW is profitable if the attacker have large attack capacity or less chance of random detection of the attacker, or the monitoring cost is low. We expect MSSW business to thrive due to the following reasons: (i) The attack capacity is continuously increasing due to the expansion of the IoT devices and network capacity. (ii) The chance of random detection is decreasing due to the fast-growing number of unprecedented types of cyber threat. (iii) The monitoring cost is expected to be lowered by increased computing power and development of machine learning.

VI. Conclusion

Cybersecurity is recognized as one of the most important challenges. In the cyber space context, we develop a game model and fully analyze the equilibrium interaction between the attacker and defender. Our game model is the first to include the optimal termination of the game in the continuous time framework, with asymmetric information and Bayesian updates. We find that the defender's expected cost explodes as the attack capacity rapidly increases, in case the defender does not realize that the attacker is strategic. This observation shows that the ISPs' strategic role of blocking suspicious users is necessary for the viability of the Internet-based society. Extending the model with monitoring cost, we provide sufficient conditions that MSSW business becomes profitable for ISPs.

Our model has possibility of many interesting extensions. For the actual application to MSSW, two directions of extension will be especially meaningful: generalization to time-dependent noise size (periodic patterns of normal actions), and consideration of multidimensional signal processes (traffic from different channels).

VII. Appendix: Proofs

A. *Heuristic derivation of differential equations for Theorem II.2*

In this subsection, we heuristically derive differential equations. The rigorous treatment of the verification argument will follow in the next subsection. We observe that the attacker's expected profit in (II.9) can be rewritten as

$$\begin{aligned}\mathbb{E}\Big[\int_0^{T\wedge\tau_p}\Delta_t dt\,\Big|\,\theta=1\Big] &= \mathbb{E}\Big[\int_0^{\tau_p} 1_{\{T>t\}}\Delta_t dt\,\Big|\,\theta=1\Big]\\ &= \mathbb{E}\Big[\int_0^{\tau_p} e^{-rt}\Delta_t dt\,\Big|\,\theta=1\Big],\end{aligned} \tag{VII.1}$$

where the second equality is from the independence of T and other random variables. Using the expression in (VII.1), we define the value function V of attacker's optimization problem as

$$V(q) = \max_{0\le(\Delta_t)_{t\in[0,\infty)}\le M} \mathbb{E}\Big[\int_0^{\tau_p} e^{-rt}\Delta_t dt \,\Big|\, \theta = 1,\, q_0 = q\Big], \tag{VII.2}$$

where $(q_t)_{t\ge0}$ is the solution of (II.8) with $dY_t = \Delta_t \cdot 1_{\{\theta=1\}}dt + \sigma\, dW_t$ and $\tau_p = \inf\{t \ge 0 :\ q_t \ge p\}$. Then Ito's formula produces the Hamilton-Jacobi-Bellman(HJB) equation, which insures that the sum of the expected change in the value function and the instantaneous profit equals zero:

$$\begin{aligned} &- rV(q) - V'(q)\cdot\tfrac{q^2(1-q)\alpha(q)^2}{\sigma^2} + \tfrac{1}{2}V''(q)\cdot\tfrac{q^2(1-q)^2\alpha(q)^2}{\sigma^2} \\ &\qquad + \max_{\Delta\in[0,M]}\big(V'(q)\cdot\tfrac{q(1-q)\alpha(q)}{\sigma^2} + 1\big)\Delta = 0, \quad \text{for } q\in(0,p). \end{aligned} \tag{VII.3}$$

When $V'(q)\cdot\frac{q(1-q)\alpha(q)}{\sigma^2} + 1 \ge 0$, $\Delta = M$ maximizes the left hand side of (VII.3). Since we expect that the maximizer in (VII.3) equals $\alpha(q)$ in equilibrium, we may rewrite the HJB equation (VII.3) for the case of $V'(q) \ge -\frac{\sigma^2}{q(1-q)M}$ as

$$\tfrac{V''(q)}{2} + \tfrac{V'(q)}{q} - \tfrac{r\sigma^2 V(q)}{M^2q^2(1-q)^2} + \tfrac{\sigma^2}{Mq^2(1-q)^2} = 0. \tag{VII.4}$$

For the case of $V'(q) < -\frac{\sigma^2}{q(1-q)M}$, we set $\alpha(q) = -\frac{\sigma^2}{q(1-q)}\cdot\frac{1}{V'(q)}$, then any $\Delta \in [0, M]$ maximizes (VII.3), and we rewrite (VII.3) as

$$\tfrac{V''(q)}{2} - \tfrac{V'(q)}{1-q} - \tfrac{r}{\sigma^2}V'(q)^2\,V(q) = 0. \tag{VII.5}$$

To set the boundary condition for V, we observe that $q = 0$ is the absorbing state in (II.8). Hence $q_0 = 0$ implies that $\tau_p = \infty$ and the attacker chooses maximum intensity M all the time. The corresponding value is $V(0) = \int_0^\infty e^{-rt}Mdt = \frac{M}{r}$. For the other extreme case, if $q_0 \ge p$, then $\tau_p = 0$ and (VII.2) implies $V(q_0) = 0$. (VII.4), (VII.5) and the previous discussion for the boundary conditions are summarized as following:

$$\begin{cases} V(0) = \frac{M}{r}, & \\ \frac{V''(q)}{2} + \frac{V'(q)}{q} - \frac{r\sigma^2V(q)}{M^2q^2(1-q)^2} + \frac{\sigma^2}{Mq^2(1-q)^2} = 0, & \text{if } V'(q) \ge -\frac{\sigma^2}{M(1-q)q} \\ \frac{V''(q)}{2} - \frac{V'(q)}{1-q} - \frac{r}{\sigma^2}V'(q)^2\,V(q) = 0, & \text{if } V'(q) < -\frac{\sigma^2}{M(1-q)q} \\ V(q) = 0, & \text{if } q\in[p,1] \end{cases} \tag{VII.6}$$

Also, the expression for α is

$$\alpha(q) = \begin{cases} M, & \text{if } q \in [0,p] \text{ and } V'(q) \geq -\frac{\sigma^2}{M(1-q)q} \\ -\frac{\sigma^2}{q(1-q)V'(q)}, & \text{if } q \in [0,p] \text{ and } V'(q) < -\frac{\sigma^2}{M(1-q)q} \\ \alpha(p), & \text{if } q \in (p,1] \end{cases} \tag{VII.7}$$

Since the game is over at τ_p, the expression (VII.7) for the case of $q \in [p,1]$ can be anything value because it is irrelevant for the attacker's optimization problem. We set $\alpha(q) = -\frac{\sigma^2}{p(1-p)V'(p)}$ in case $q \in [p,1]$, for the continuity of α at $q = p$ (see Definition II.1).

Now we derive a differential equation from the defender's optimal stopping problem (II.10). Using (II.8) and the independence of T, the defender's expected cost can be rewritten as (we will check this in the next subsection rigorously)

$$\mathbb{E}\Big[\int_0^\tau e^{-rt}\alpha(q_t)q_t\,dt + e^{-r\tau}l_f \cdot (1-q_\tau)\Big]. \tag{VII.8}$$

Therefore, we define the defender's value function U as

$$U(q) = \min_{\tau \in \mathcal{T}} \mathbb{E}\Big[\int_0^\tau e^{-rt}\alpha(q_t)q_t\,dt + e^{-r\tau}l_f \cdot (1-q_\tau) \,\Big|\, q_0 = q\Big] \tag{VII.9}$$

where $(q_t)_{t\geq 0}$ is the solution of (II.8) with $dY_t = \alpha(q_t)\cdot 1_{\{\theta=1\}}dt + \sigma\, dW_t$ and $\tau_p = \inf\{t \geq 0 :\ q_t \geq p\}$, and $\mathcal{T}$ be the set of all stopping times with respect to the filtration $(\mathcal{F}_t^Y)_{t\geq 0}$. Application of Ito's formula to the optimal stopping problem (VII.9) produces the following variational inequality:[21]

$$\min\Big\{ -rU(q) + \tfrac{1}{2}U''(q)\cdot\tfrac{q^2(1-q)^2\alpha(q)^2}{\sigma^2} + q\,\alpha(q)\,,\ l_f(1-q) - U(q)\Big\} = 0, \tag{VII.10}$$

with the optimal stopping time of the following form:

$$\tau^* = \inf\{t \geq 0 : U(q_t) = l_f(1-q_t)\}$$

In equilibrium, we expect τ_p to be the optimal stopping time. To set the boundary condition of (VII.10), we observe that $q_0 = 0$ implies $\theta = 0$ and $q_t \equiv 0$ all the time according to (II.8). In this case, $\tau_p = \infty$ and $U(0) = 0$. On the other hand, the smooth-fit principle imposes another side of boundary conditions, $U(p-) = l_f(1-p)$ and $U'(p-) = -l_f$. Based on this discussion, we may rewrite

[21] The form of the variational inequality and optimal stopping time is standard in the literature on optimal stopping problems. See [Huyen Pham] Chapter 5.2, for details.

(VII.10) with boundary conditions as following.

$$\text{(VII.11)} \qquad \text{If } q \in [0,p), \quad \begin{cases} -rU(q) + \frac{q^2(1-q)^2\alpha(q)^2U''(q)}{2\sigma^2} + q\,\alpha(q) = 0, \\ U(q) < l_f(1-q). \end{cases}$$

$$\text{(VII.12)} \qquad \text{If } q \in [p,1], \quad \begin{cases} -rU(q) + \frac{q^2(1-q)^2\alpha(q)^2U''(q)}{2\sigma^2} + q\,\alpha(q) \geq 0, \\ U(q) = l_f(1-q). \end{cases}$$

$$\text{(VII.13)} \qquad U(0) = 0, \quad U(p-) = l_f(1-p), \quad U'(p-) = -l_f.$$

B. Solution of the differential equations

In Proposition VII.2, we provide the explicit solutions V, U, α, p of the system (VII.6), (VII.7) and (VII.11)-(VII.13). For convenience, we define functions φ, y and constants a, b, c, q^* as follows:

$$\text{(VII.14)} \qquad \begin{aligned} \varphi(x) &:= \tfrac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt \\ a &:= \tfrac{1}{2}\Big(\sqrt{1 + \tfrac{8r\sigma^2}{M^2}} - 1\Big) \\ b &:= \tfrac{(1-a)M}{2\sigma\sqrt{r}} \\ c &:= \tfrac{2\sigma\sqrt{r}e^{-b^2}}{M\sqrt{\pi}} + \varphi(b) \\ q^* &:= \tfrac{p(c-\varphi(b))}{c - p\,\varphi(b)} \\ y(x) &:= \varphi^{-1}\big(\tfrac{c(p-x)}{p(1-x)}\big) \end{aligned}$$

In (VII.14), q^* and y depends on a constant $p \in (0,1)$ which will be determined later in Proposition VII.2. To deal with the inequalities in the system, we obtain the following lemma.

LEMMA VII.1: *If $\frac{r\sigma^2}{M^2} < 1$, then the followings hold.*

(1) $a \in (0,1)$, $b > 0$, $c > 0$, $q^* \in (0,p)$ and $y(q^*) = b$.

(2) $0 < c\sqrt{\pi}\,\big(\frac{(1-p)x}{p(1-x)}\big)e^{y(x)^2} - \frac{2\sigma\sqrt{r}}{M}$ for $x \in (q^*, p]$.

PROOF:

(1) This is from elementary calculation with the underlying assumption $\frac{r\sigma^2}{M^2} < 1$.

(2) Observe that $z \mapsto \varphi(z) + \frac{2\sigma\sqrt{r}\,e^{-z^2}}{M\sqrt{\pi}}$ is strictly increasing on $z \in [0,b]$. For $x \in (q^*, p]$, we observe that $y(x) < b$ and

$$\varphi(b) + \tfrac{2\sigma\sqrt{r}\,e^{-b^2}}{M\sqrt{\pi}} > \varphi(y(x)) + \tfrac{2\sigma\sqrt{r}\,e^{-y(x)^2}}{M\sqrt{\pi}} = \Big(\tfrac{2\sigma\sqrt{r}\,e^{-y(x)^2}}{M\sqrt{\pi}} - \tfrac{c(1-p)x}{p(1-x)}\Big) + c.$$

The above inequality, together with the expression of c, produces (2).

PROPOSITION VII.2: *(1) If* $\frac{r\sigma^2}{M^2} \geq 1$, *then the unique solution of the system* (VII.6), (VII.7) *and* (VII.11)-(VII.13) *is given by following:*

$$V(q) = \begin{cases} \frac{M}{r}\big(1 - \big(\frac{1-p}{p}\big)^a \big(\frac{q}{1-q}\big)^a\big), & \text{if } q \in [0,p) \\ 0, & \text{if } q \in [p,1] \end{cases} \tag{VII.15}$$

$$\alpha(q) = M, \quad \text{if } q \in [0,1] \tag{VII.16}$$

$$U(q) = \begin{cases} q\Big(\frac{M}{r} - \big(\frac{M}{r} - \frac{(1-p)l_f}{p}\big)\big(\frac{1-p}{p}\big)^a \big(\frac{q}{1-q}\big)^a\Big), & \text{if } q \in [0,p) \\ (1-q)l_f, & \text{if } q \in [p,1] \end{cases} \tag{VII.17}$$

$$p = \frac{(1+a)r\, l_f}{(1+a)r\, l_f + aM} \tag{VII.18}$$

The solution satisfy $V \in C^2([0,p))$, $U \in C^1([0,1]) \cup C^2([0,1] \setminus \{p\})$ *and* $\alpha \in C([0,1])$.

(2) If $\frac{r\sigma^2}{M^2} < 1$, *then the unique solution of the system* (VII.6), (VII.7) *and* (VII.11)-(VII.13) *is given by following:*

(VII.19)

$$V(q) = \begin{cases} \frac{M}{r} - \frac{\sigma^2}{aM}\big(\frac{1-q^*}{q^*}\big)^a \big(\frac{q}{1-q}\big)^a, & \text{if } q \in [0,q^*] \\ \frac{\sigma}{\sqrt{r}}\, y(q), & \text{if } q \in (q^*,p) \\ 0, & \text{if } q \in [p,1] \end{cases}$$

(VII.20)

$$\alpha(q) = \begin{cases} M, & \text{if } q \in [0,q^*] \\ \frac{2p(1-q)\sigma\sqrt{r}}{c\sqrt{\pi}\,(1-p)q}\, e^{-y(q)^2}, & \text{if } q \in (q^*,p) \\ \frac{2\sigma\sqrt{r}}{c\sqrt{\pi}}, & \text{if } q \in [p,1] \end{cases}$$

(VII.21)

$$U(q) = \begin{cases} q\Big(\frac{M}{r} - \big(\frac{\sigma^2}{aM} - \frac{c\sqrt{\pi r}(1-p)l_f\sigma}{(1+a)Mp}\big)\big(\frac{1-q^*}{q^*}\big)^a \big(\frac{q}{1-q}\big)^a\Big), & \text{if } q \in [0,q^*] \\ \frac{\sigma}{\sqrt{r}}\, q\, y(q) + l_f(1-q)\big(e^{-y(q)^2} - \frac{c\sqrt{\pi}(1-p)q\, y(q)}{p(1-q)}\big), & \text{if } q \in (q^*,p) \\ (1-q)l_f, & \text{if } q \in [p,1] \end{cases}$$

$$p = \frac{cl_f\sqrt{\pi r}}{cl_f\sqrt{\pi r} + \sigma} \tag{VII.22}$$

The solution satisfy $V \in C^2([0,p))$, $U \in C^1([0,1]) \cup C^2([0,1] \setminus \{p\})$ *and* $\alpha \in C([0,1])$.

PROOF:

We prove (1) and (2) at the same time. First, to obtain the expression for V, we observe that the solutions of the following two differential equations

$$\begin{cases} \frac{V''(q)}{2} + \frac{V'(q)}{q} - \frac{r\sigma^2 V(q)}{M^2 q^2 (1-q)^2} + \frac{\sigma^2}{Mq^2(1-q)^2} = 0 \quad \text{with} \quad V(0) = \frac{M}{r} \\ \frac{V''(q)}{2} - \frac{V'(q)}{1-q} - \frac{r}{\sigma^2} V'(q)^2 V(q) = 0 \quad \text{with} \quad V(p) = 0 \end{cases} \tag{VII.23}$$

are given by[22]

$$V(q) = \begin{cases} \frac{M}{r}\Big(1 - C_1 \cdot \big(\frac{q}{1-q}\big)^a\Big) \\ \frac{\sigma}{\sqrt{r}}\,\varphi^{-1}\big(C_2 \cdot \frac{p-q}{1-q}\big) \end{cases} \quad \text{repectively,} \tag{VII.24}$$

where C_1 and C_2 are constants. We determine the constants C_1 and C_2 uniquely by the value matching and smooth pasting conditions, and obtain the following formula for V:

$$\text{If } \tfrac{r\sigma^2}{M^2} \geq 1, \quad V(q) = \begin{cases} \frac{M}{r}\big(1 - \big(\frac{1-p}{p}\big)^a\big(\frac{q}{1-q}\big)^a\big), & q \in [0,p) \\ 0, & q \in [p,1] \end{cases} \tag{VII.25}$$

$$\text{If } \tfrac{r\sigma^2}{M^2} < 1, \quad V(q) = \begin{cases} \frac{M}{r} - \frac{\sigma^2}{aM}\big(\frac{1-q^*}{q^*}\big)^a\big(\frac{q}{1-q}\big)^a, & q \in [0,q^*] \\ \frac{\sigma}{\sqrt{r}}\,y(q), & q \in (q^*,p) \\ 0, & q \in [p,1] \end{cases} \tag{VII.26}$$

Lemma VII.1 (1) ensures that V in (VII.25) and (VII.26) are well-defined. We need to check that (VII.25) and (VII.26) satisfy (VII.6) and $V \in C^2([0,p))$. In case $\frac{r\sigma^2}{M^2} \geq 1$, we observe that $a \leq \frac{r\sigma^2}{M^2}$ and this implies that V in (VII.25) satisfies $V'(q) \geq -\frac{\sigma^2}{M(1-q)q}$ for $q \in [0,p)$. In case $\frac{r\sigma^2}{M^2} < 1$, Lemma VII.1 implies that V in (VII.26) satisfies

$$\begin{cases} V'(q) + \frac{\sigma^2}{M(1-q)q} = \frac{\sigma^2}{M(1-q)q} \cdot \Big(1 - \big(\frac{1-q^*}{q^*}\big)^a\big(\frac{q}{1-q}\big)^a\Big) \geq 0, & q \in [0,q^*] \\ V'(q) + \frac{\sigma^2}{M(1-q)q} = -\frac{\sigma}{2\sqrt{r}(1-q)q}\Big(c\sqrt{\pi}\,\big(\frac{(1-p)q}{p(1-q)}\big)e^{y(q)^2} - \frac{2\sigma\sqrt{r}}{M}\Big) < 0, & q \in (q^*,p) \end{cases}$$

and solves the corresponding differential equations in (VII.6). Also, the continuity of V, V' and V'' at $q = q^*$ are given by

$$\begin{cases} V(q^*-) = V(q^*+) = \frac{M}{r} - \frac{\sigma^2}{aM} \\ V'(q^*-) = V'(q^*+) = -\frac{\sigma^2}{M(1-q^*)q^*} \\ V''(q^*-) = V''(q^*+) = -\frac{\sigma^2(2q^*+a-1)}{M((1-q^*)q^*)^2} \end{cases} \tag{VII.27}$$

Therefore, we conclude that if $\frac{r\sigma^2}{M^2} \geq 1$ (resp., $\frac{r\sigma^2}{M^2} < 1$), (VII.25) (resp., (VII.26)) is the unique solution of (VII.6) with the desired smoothness.

Next, the function α in (VII.7) is rewritten as (VII.16) and (VII.20), by straightforward calculations using the expressions (VII.25) and (VII.26).

Now we find solution U of (VII.11)-(VII.13). When α is as in (VII.16) (resp.,

[22]To solve the second differential equation, it is helpful to change variable as $x = \frac{p-q}{p(1-q)}$

(VII.20)), the following system of equations

$$\begin{cases} U(0) = 0 \\ -rU(q) + \frac{q^2(1-q)^2\alpha(q)^2U''(q)}{2\sigma^2} + q\,\alpha(q) = 0, & q \in [0,p) \\ U(q) = (1-q)l_f, & q \in [p,1] \end{cases}$$

has the unique explicit solution (VII.17) (resp., (VII.21)). As in (VII.27), direct computation shows that $U(p-) = l_f(1-p)$ and U has continuous second derivative on $[0,p)$. Now the only remaining conditions to be checked are

$$U'(p-) = -l_f, \tag{VII.28}$$

$$U(q) < l_f(1-q) \text{ for } q \in [0,p), \tag{VII.29}$$

$$-rU(q) + \frac{q^2(1-q)^2\alpha(q)^2U''(q)}{2\sigma^2} + q\,\alpha(q) \geq 0 \text{ for } q \in [p,1]. \tag{VII.30}$$

We solve (VII.28) for p, using the expression (VII.17) (resp., (VII.21)), and obtain (VII.18) (resp., (VII.22)). One can easily see that $p \in (0,1)$.

To check (VII.29), it is enough to observe that $U(p-) = l_f(1-p)$, $U'(p-) = -l_f$ and U is strictly concave on $[0,p)$. Indeed, we use (VII.17), (VII.21), (VII.18) and (VII.22) to observe that for $q \in [0,p)$,

$$U''(q) = \begin{cases} -\frac{aM}{r(1-q)^2q} \cdot \left(\frac{aM}{(1+a)rl_f}\right)^a \left(\frac{q}{1-q}\right)^a, & \text{if } \frac{r\sigma^2}{M^2} \geq 1 \text{ and } q \in (0,p) \\ -\frac{1}{M(1-q)^2q} \cdot \left(\frac{1-q^*}{q^*}\right)^a \left(\frac{q}{1-q}\right)^a, & \text{if } \frac{r\sigma^2}{M^2} < 1 \text{ and } q \in (0,q^*] \\ -\frac{\sigma^2}{2l_fr(1-q)^3} e^{y(q)^2}, & \text{if } \frac{r\sigma^2}{M^2} < 1 \text{ and } q \in (q^*,p) \end{cases} \tag{VII.31}$$

and conclude that U is strictly concave on $[0,p)$.

Finally, to check (VII.30), we observe that (VII.16)-(VII.18) and (VII.20)-(VII.22) imply following: For $q \in [p,1]$,

$$-rU(q) + \frac{q^2(1-q)^2\alpha(q)^2U''(q)}{2\sigma^2} + q\,\alpha(q) \geq \begin{cases} \frac{l_frM}{l_fr+a(M+l_fr)} > 0, & \text{if } \frac{r\sigma^2}{M^2} \geq 1 \\ \frac{l_fr\sigma}{l_fc\sqrt{\pi r}+\sigma} > 0, & \text{if } \frac{r\sigma^2}{M^2} < 1 \end{cases}$$

C. *Proof of Theorem II.2 (verification)*

Proposition VII.2 provides the explicit form of the unique solution V, α, U and p of the system (VII.6), (VII.7) and (VII.11)-(VII.13). Our goal in this subsection is to verify that (p,α) is an equilibrium in Definition II.1.

THEOREM VII.3: *(p,α) defined in Proposition VII.2 is a Baysian Nash equilibrium in Definition II.1.*

PROOF:

Checking (1) in Definition II.1

In this part of the proof, we use notation $q_t^{(\Delta)}$ and $\tau_p^{(\Delta)}$ instead of q_t and τ_p, to emphasize their dependence on the attacker's strategy Δ. To be specific, for attack-intensity process $(\Delta_t)_{t\in[0,\infty)}$ such that $0 \le \Delta_t \le M$, let the process $(q_t^{(\Delta)})_{t\in[0,\infty)}$ be the solution of the adjustment formula (II.8) with initial value q_0, and $\tau_p^{(\Delta)} = \inf\{t \ge 0 : q_t^{(\Delta)} \ge p\}$.

To verify that V in Proposition VII.2 is the attacker's value function, we apply Ito's formula with $\theta = 1$: For $q_0 \in [0, p]$,

(VII.32)

$$
\begin{aligned}
&e^{-r(t\wedge\tau_p^{(\Delta)})}V(q^{(\Delta)}_{t\wedge\tau_p^{(\Delta)}}) + \int_0^{t\wedge\tau_p^{(\Delta)}} e^{-rs}\Delta_s ds \\
&= V(q_0) + \int_0^{t\wedge\tau_p^{(\Delta)}} e^{-rs}\Big(- rV(q_s^{(\Delta)})ds + V'(q_s^{(\Delta)})dq_s^{(\Delta)} + \frac{1}{2}V''(q_s^{(\Delta)})d\langle q^{(\Delta)}\rangle_s + \Delta_s ds\Big) \\
&= V(q_0) + \int_0^{t\wedge\tau_p^{(\Delta)}} e^{-rs}\Big(- rV(q) - V'(q)\cdot\tfrac{q^2(1-q)\alpha(q)^2}{\sigma^2} + \tfrac{1}{2}V''(q)\cdot\tfrac{q^2(1-q)^2\alpha(q)^2}{\sigma^2} \\
&\qquad + \big(V'(q)\cdot\tfrac{q(1-q)\alpha(q)}{\sigma^2} + 1\big)\Delta_s\Big)\Big|_{q=q_s^{(\Delta)}} ds + \int_0^{t\wedge\tau_p^{\Delta}} e^{-rs}\,\tfrac{q(1-q)\alpha(q)V'(q)}{\sigma}\Big|_{q=q_s^{(\Delta)}} dW_s \\
&\le V(q_0) + \int_0^{t\wedge\tau_p^{\Delta}} e^{-rs}\,\tfrac{q(1-q)\alpha(q)V'(q)}{\sigma}\Big|_{q=q_s^{(\Delta)}} dW_s,
\end{aligned}
$$

where the last equality above is due to (VII.3). Indeed, V in Proposition VII.2 satisfies (VII.6), and (VII.6) implies (VII.3).

We observe that $\frac{q(1-q)\alpha(q)V'(q)}{\sigma}$ is bounded on $q \in [0, p]$. Then the stochastic integral term in (VII.32) is a square-integrable martingale and has mean zero. This observation and (VII.32) produce

(VII.33)

$$
\begin{aligned}
&\mathbb{E}\Big[e^{-r(t\wedge\tau_p^{(\Delta)})}V(q^{(\Delta)}_{t\wedge\tau_p^{(\Delta)}}) + \int_0^{t\wedge\tau_p^{(\Delta)}} e^{-rs}\Delta_s ds \,\Big|\, \theta = 1\Big] \\
&\le V(q_0) = \mathbb{E}\Big[e^{-r(t\wedge\tau_p^{(\alpha)})}V(q^{(\alpha)}_{t\wedge\tau_p^{(\alpha)}}) + \int_0^{t\wedge\tau_p^{(\alpha)}} e^{-rs}\alpha(q_s^{(\alpha)})ds \,\Big|\, \theta = 1\Big],
\end{aligned}
$$

where the equality is due to the fact that the maximum value is achieved at $\Delta = \alpha(q)$ in (VII.3). Here, we denote $q_t^{(\alpha)}$ and $\tau_p^{(\alpha)}$ as the belief process and stopping time with $\Delta_t = \alpha(q_t^{(\alpha)})$. Since V is bounded on its domain, as $t \to \infty$,

the bounded convergence theorem and (VII.33) imply

$$\begin{aligned}(\text{VII.34}) \qquad &\mathbb{E}\Big[e^{-r\tau_p^{(\Delta)}}V(q_{\tau_p^{(\Delta)}}) + \int_0^{\tau_p^{(\Delta)}} e^{-rs}\Delta_s ds \,\Big|\, \theta = 1\Big] \\ &\le V(q_0) = \mathbb{E}\Big[e^{-r\tau_p^{(\alpha)}}V(q^{(\alpha)}_{\tau_p}) + \int_0^{\tau_p^{(\alpha)}} e^{-rs}\alpha(q_s^{(\alpha)})ds \,\Big|\, \theta = 1\Big].\end{aligned}$$

$V(p) = 0$ implies that $V(q_{\tau_p^{(\Delta)}}) \cdot 1_{\{\tau_p^{(\Delta)}<\infty\}} = 0$. Therefore, (VII.34) produces

$$(\text{VII.35}) \quad \mathbb{E}\Big[\int_0^{\tau_p^{(\Delta)}} e^{-rs}\Delta_s ds \,\Big|\, \theta = 1\Big] \le V(q_0) = \mathbb{E}\Big[\int_0^{\tau_p^{(\alpha)}} e^{-rs}\alpha(q_s^{(\alpha)})ds \,\Big|\, \theta = 1\Big].$$

Finally, we conclude (II.9) by (VII.1) and (VII.35).

Checking (2) in Definition II.1

In this part of the proof, the underlying assumption is $\Delta_t = \alpha(q_t)$. We first check that the solution of (II.8) satisfies $q_t = \mathbb{E}[\theta|\mathcal{F}_t^Y]$. When $\Delta_t = \alpha(q_t)$, the adjustment formula (II.8) becomes

$$(\text{VII.36}) \qquad dq_t = \tfrac{q_t(1-q_t)\alpha(q_t)}{\sigma^2}\Big(\alpha(q_t)\big(1_{\{\theta=1\}} - q_t\big)\,dt + \sigma dW_t\Big), \quad t \in [0,\infty).$$

Since α is Lipschitz continuous and bounded, the standard existence and uniqueness result[23] of the solution of SDE implies that there exists a unique solution q_t of (VII.36) with initial value q_0.

Let $\hat{q}_t := \mathbb{E}[\theta|\mathcal{F}_t^Y]$ with $Y_t = \big(\int_0^t \alpha(q_t)dt\big)\cdot 1_{\{\theta=1\}} + \int_0^t \sigma\, dW_t$. Then [Lipster and Shiriyaev Theorem 8.1] implies that $\hat{q}_t$ satisfies the following SDE:

$$(\text{VII.37}) \qquad d\hat{q}_t = \tfrac{\hat{q}_t(1-\hat{q}_t)\alpha(q_t)}{\sigma^2}\Big(\alpha(q_t)\big(1_{\{\theta=1\}} - \hat{q}_t\big)\,dt + \sigma dW_t\Big), \quad t \in [0,\infty).$$

Since the coefficients in the above SDE are bounded and Lipschitz in $\hat{q}$, (VII.37) has a unique solution with initial value q_0. (VII.36) implies that q_t is also a solution of (VII.37), and we conclude that

$$(\text{VII.38}) \qquad q_t = \hat{q}_t = \mathbb{E}[\theta|\mathcal{F}_t^Y].$$

Now we prove (II.10). Let τ be any stopping time with respect to the filtration

[23]For example, see Pham Chapter 1.3.

$(\mathcal{F}_t^Y)_{t\geq 0}$. Then,

$$
\begin{aligned}
&e^{-r(t\wedge\tau)}U(q_{t\wedge\tau}) + \int_0^{t\wedge\tau} e^{-rs}\alpha(q_s)q_s\,ds \\
&= U(q_0) + \int_0^{t\wedge\tau} e^{-rs}\Big(- rU(q_s) + \tfrac{q_s^2(1-q_s)^2\alpha(q_s)^2}{2\sigma^2}U''(q_s) + q_s\,\alpha(q_s)\Big)ds \\
&\qquad + \int_0^{t\wedge\tau} e^{-rs}U'(q_s)dq_s \\
&\geq U(q_0) + \int_0^{t\wedge\tau} e^{-rs}U'(q_s)dq_s,
\end{aligned}
\tag{VII.39}
$$

where Ito's formula produces the equality and the inequality is due to (VII.10). Indeed, U in Proposition VII.2 satisfies (VII.11)-(VII.13) which imply (VII.10). Similarly, if we consider the stopping time τ_p, Ito's formula and (VII.11)-(VII.13) produce

$$
e^{-r(t\wedge\tau_p)}U(q_{t\wedge\tau_p}) + \int_0^{t\wedge\tau_p} e^{-rs}\alpha(q_s)q_s\,ds = U(q_0) + \int_0^{t\wedge\tau_p} e^{-rs}U'(q_s)dq_s.
\tag{VII.40}
$$

Using (VII.38) and iterated conditioning, we obtain

$$
\begin{aligned}
&\mathbb{E}\Big[\int_0^{t\wedge\tau} e^{-rs}U'(q_s)dq_s\Big] \\
&= \int_0^{\infty} \mathbb{E}\Big[1_{\{0\leq s\leq t\wedge\tau\}}e^{-rs}U'(q_s)\tfrac{q_s(1-q_s)\alpha(q_s)^2}{\sigma^2}\mathbb{E}\big[1_{\{\theta=1\}} - q_s\big|\mathcal{F}_s^Y\big]\Big]ds \\
&\qquad + \mathbb{E}\Big[\int_0^{t\wedge\tau} e^{-rs}U'(q_s)\tfrac{q_s(1-q_s)\alpha(q_s)}{\sigma}dW_s\Big] \\
&= 0.
\end{aligned}
\tag{VII.41}
$$

The first equality above is due to the Fubini's theorem and the boundedness of U', and the second equality holds because $\frac{U'(q)q(1-q)\alpha(q)}{\sigma}$ is bounded on $q\in[0,1]$ and the stochastic integral part is a square-integrable martingale.
Now we combine (VII.39), (VII.40) and (VII.41) into the following:

$$
\begin{aligned}
&\mathbb{E}\Big[e^{-r(t\wedge\tau)}U(q_{t\wedge\tau}) + \int_0^{t\wedge\tau} e^{-rs}\alpha(q_s)q_s\,ds\Big] \\
&\geq U(q_0) = \mathbb{E}\Big[e^{-r(t\wedge\tau_p)}U(q_{t\wedge\tau_p}) + \int_0^{t\wedge\tau_p} e^{-rs}\alpha(q_s)q_s\,ds\Big]
\end{aligned}
\tag{VII.42}
$$

The boundedness of U and α enable us to apply the dominated convergence

theorem to (VII.42) for $t \to \infty$:

$$\begin{aligned} &\mathbb{E}\Big[e^{-r\tau}U(q_\tau) + \int_0^\tau e^{-rs}\alpha(q_s)q_s\,ds\Big] \\ &\geq U(q_0) = \mathbb{E}\Big[e^{-r\tau_p}U(q_{\tau_p}) + \int_0^{\tau_p} e^{-rs}\alpha(q_s)q_s\,ds\Big] \end{aligned} \tag{VII.43}$$

(VII.11)-(VII.13) and (VII.43) imply that

$$\begin{aligned} &\mathbb{E}\Big[e^{-r\tau}l_f(1-q_\tau) + \int_0^\tau e^{-rs}\alpha(q_s)q_s\,ds\Big] \\ &\geq \mathbb{E}\Big[e^{-r\tau_p}l_f(1-q_{\tau_p}) + \int_0^{\tau_p} e^{-rs}\alpha(q_s)q_s\,ds\Big] \end{aligned} \tag{VII.44}$$

It remains to derive (II.10) from (VII.44). Since the process $(q_t)_{t\in[0,\infty)}$ is uniformly bounded, we can apply the optional sampling theorem[24] to (VII.38) and obtain

$$q_\tau = \mathbb{E}[\theta|\mathcal{F}_\tau^Y] = \mathbb{E}[1_{\{\theta=1\}}|\mathcal{F}_\tau^Y]. \tag{VII.45}$$

Recall that τ is a stopping time with respect to $(\mathcal{F}_t^Y)_{t\in[0,\infty)}$, and T is independent of $(\mathcal{F}_t^Y)_{t\in[0,\infty)}$ and θ. This implies

$$\mathbb{E}[1_{\{T>\tau\}}|\mathcal{F}_\tau^Y, \theta] = e^{-r\tau}. \tag{VII.46}$$

Using (VII.45) and (VII.46), we check the following equalities:

$$\begin{aligned} &\mathbb{E}\Big[e^{-r\tau}l_f(1-q_\tau) + \int_0^\tau e^{-rs}\alpha(q_s)q_s\,ds\Big] \\ &= \mathbb{E}\Big[l_f\cdot e^{-r\tau}1_{\{\theta=0\}}\Big] + \int_0^\infty \mathbb{E}\Big[1_{\{s<\tau\}}e^{-rs}\alpha(q_s)1_{\{\theta=1\}}\Big]\,ds \\ &= \mathbb{E}\Big[l_f\cdot 1_{\{\theta=0\}}1_{\{T>\tau\}}\Big] + \int_0^\infty \mathbb{E}\Big[1_{\{s<\tau\}}1_{\{s<T\}}\alpha(q_s)1_{\{\theta=1\}}\Big]\,ds \\ &= \mathbb{E}\Big[\Big(\int_0^{T\wedge\tau}\alpha(q_s)ds\Big)\cdot 1_{\{\theta=1\}} + l_f\cdot 1_{\{\theta=0,\,\tau<T\}}\Big], \end{aligned} \tag{VII.47}$$

where we apply the Fubini theorem for the first and third equality, and use the iterated conditioning for the first and second equality.

In summary, (VII.44) and (VII.47) hold for any $(\mathcal{F}_t^Y)_{t\in[0,\infty)}$ stopping time τ, and this implies (II.10).

[24]See, for example, Karatzas & Shreve Theorem 3.22 in Chapter 1.

D. Proof of Propositions in Section III

Proof of Proposition III.1: The following proposition includes Proposition III.1.

PROPOSITION VII.4: *Assume that the attacker and defender behave as followings:*
(i) The attacker is not strategic and chooses $\Delta_t = M$ for all $t \geq 0$.
(ii) The defender knows that the attacker is non-strategic (in case the user is attacker), and optimally blocks the user to minimize the expected cost,

$$\min_{\tau\in\mathcal{T}} \mathbb{E}\Big[\Big(\int_0^{T\wedge\tau} M ds\Big)\cdot 1_{\{\theta=1\}} + l_f \cdot 1_{\{\theta=0,\,\tau<T\}}\Big]. \tag{VII.48}$$

Then, the optimal blocking strategy $\tau_{\tilde{p}}$, and the corresponding defender's minimal expected cost $C_2(q_0)$ and the attacker's expected profit $V_2(q_0)$ are

$$\begin{aligned} &\tau_{\tilde{p}} = \inf\{t \geq 0 : q_t \geq \tilde{p}\} \quad \textit{with} \quad \tilde{p} = \tfrac{(1+a)r\,l_f}{(1+a)r\,l_f + aM}, \\ &C_2(q_0) = \begin{cases} q_0\Big(\frac{M}{r} - \big(\frac{M}{r} - \frac{(1-\tilde{p})l_f}{\tilde{p}}\big)\big(\frac{1-\tilde{p}}{\tilde{p}}\big)^a\big(\frac{q_0}{1-q_0}\big)^a\Big), & \textit{if } \ q_0 \in [0,\tilde{p}) \\ (1-q_0)l_f, & \textit{if } \ q_0 \in [\tilde{p},1] \end{cases} \\ &V_2(q_0) = \begin{cases} \frac{M}{r}\big(1 - \big(\frac{1-\tilde{p}}{\tilde{p}}\big)^a\big(\frac{q_0}{1-q_0}\big)^a\big), & \textit{if } \ q_0 \in [0,\tilde{p}) \\ 0, & \textit{if } \ q_0 \in [\tilde{p},1] \end{cases} \end{aligned} \tag{VII.49}$$

where the process $(q_t)_{t\in[0,\infty)}$ is the unique solution of (II.3) *with $\Delta_t = M$, and the constant a is defined in* (VII.14)*. Also,* (III.2) *holds.*

PROOF:
We observe that C_2 and V_2 in (VII.49) satisfy following differential equations:

$$0 = \min\Big\{q\,M - rC_2(q) + \tfrac{1}{2}C_2''(q)\tfrac{q^2(1-q)^2M^2}{\sigma^2}\,,\ l_f(1-q) - C_2(q)\Big\} \tag{VII.50}$$

$$0 = M - rV_2(q) - V_2'(q)\tfrac{q(1-q)^2M^2}{\sigma^2} + \tfrac{1}{2}V_2''(q)\tfrac{q^2(1-q)^2M^2}{\sigma^2} \quad \text{for } q \in [0,p) \tag{VII.51}$$

Consider a stopping time $\tau \in \mathcal{T}$. Using (VII.50) and following the procedure (VII.39)-(VII.47) in the current setup, we obtain

$$\begin{aligned} &\mathbb{E}\Big[\Big(\int_0^{T\wedge\tau} M dt\Big)\cdot 1_{\{\theta=1\}} + l_f \cdot 1_{\{\theta=0,\,\tau<T\}}\Big] \\ &\geq C_2(q_0) = \mathbb{E}\Big[\Big(\int_0^{T\wedge\tau_{\tilde{p}}} M\,dt\Big)\cdot 1_{\{\theta=1\}} + l_f \cdot 1_{\{\theta=0,\,\tau_{\tilde{p}}<T\}}\Big] \end{aligned} \tag{VII.52}$$

Obviously, (VII.52) implies that $\tau_{\tilde{p}}$ (resp., C_2) in (VII.49) is the optimal blocking strategy (resp., defender's minimal expected cost).

Now we check that V_2 in (VII.49) is the attacker's expected profit. When $\theta = 1$ and $q_0 \in [0, \tilde{p}]$, the Ito's formula and (VII.51) produces

(VII.53)
$$\begin{aligned} & e^{-r(t\wedge\tau_{\tilde{p}})}V_2(q_{t\wedge\tau_{\tilde{p}}}) + \int_0^{t\wedge\tau_{\tilde{p}}} e^{-rs}Mds \\ &= V_2(q_0) + \int_0^{t\wedge\tau_{\tilde{p}}} e^{-rs}\Big(\big(M - rV_2(q_s)\big)ds + V_2'(q_s)dq_s + \frac{1}{2}V_2''(q_s)d\langle q\rangle_s\Big) \\ &= V_2(q_0) + \int_0^{t\wedge\tau_{\tilde{p}}} e^{-rs}V_2'(q_s)\tfrac{q_s(1-q_s)M}{\sigma^2}dW_s. \end{aligned}$$

We observe that $\frac{q(1-q)\alpha(q)V_2'(q)}{\sigma}$ is bounded on $q \in [0, \tilde{p}]$. Then the stochastic integral term in (VII.53) is a square-integrable martingale and has mean zero. This observation and (VII.53) produce

(VII.54)
$$\begin{aligned} V_2(q_0) &= \mathbb{E}\Big[e^{-r(t\wedge\tau_{\tilde{p}})}V_2(q_{t\wedge\tau_{\tilde{p}}}) + \int_0^{t\wedge\tau_{\tilde{p}}} e^{-rs}Mds \,\Big|\, \theta = 1\Big] \\ &\to \mathbb{E}\Big[e^{-r\tau_{\tilde{p}}}V_2(q_{\tau_{\tilde{p}}}) + \int_0^{\tau_{\tilde{p}}} e^{-rs}Mds \,\Big|\, \theta = 1\Big] \quad \text{as } t \to \infty \\ &= \mathbb{E}\Big[\int_0^{T\wedge\tau_{\tilde{p}}} Mds \,\Big|\, \theta = 1\Big], \end{aligned}$$

where the convergence is due to the boundedness of V_2 and the dominated convergence theorem, and the last equality is due to the observation $V_2(q_{\tau_{\tilde{p}}})\cdot 1_{\{\tau_{\tilde{p}}<\infty\}} = 0$.

Finally, suitable use of LHospital's rule and $a = \mathcal{O}(\frac{1}{M^2})$ for large M produce (III.2).

Proof of Proposition III.2: The following proposition includes Proposition III.2.

PROPOSITION VII.5: *Assume that the attacker and defender behave as followings:*
(i) The attacker is strategic and knows that the defender applies the blocking strategy $\tau_{\tilde{p}}$ in Proposition VII.49. Here, $(q_t)_{t\in[0,\infty)}$ is the solution of the following SDE,

(VII.55) $$dq_t = \frac{q_t(1-q_t)M}{\sigma^2}\Big(dY_t - q_tMdt\Big) \quad \textit{with} \quad dY_t = \Delta_t 1_{\{\theta=1\}}dt + \sigma\, dW_t,$$

where $(\Delta_t)_{t\in[0,\infty)}$ is the attackers possible strategy. The attacker optimally chooses the strategy to maximize the expected profit,

(VII.56) $$\big(\tilde{\alpha}(q_t)\big)_{t\geq 0} \in \underset{0\leq(\Delta_t)_{t\in[0,\infty)}\leq M}{\arg\max}\ \mathbb{E}\Big[\int_0^{T\wedge\tau_{\tilde{p}}} \Delta_t dt \,\Big|\, \theta = 1\Big].$$

(ii) The defender thinks that the attacker is no-strategic as in Proposition VII.4. Consequently, the defender applies the blocking strategy $\tau_{\tilde{p}}$ in Proposition VII.49 where $(q_t)_{t\in[0,\infty)}$ is the solution of (VII.55) *with* $\Delta_t = \tilde{\alpha}(q_t)$ *in* (VII.56).

Then, the attacker's optimal strategy $\tilde{\alpha}$, and the corresponding attacker's maximal expected profit $V_3(q_0)$ and the defender's expected cost $C_3(q_0)$ are

(VII.57)
$$\bullet \text{ If } \tfrac{r\sigma^2}{M^2} \geq 1:$$
$$V_3(q_0) = \begin{cases} \frac{M}{r}\big(1 - (\frac{1-\tilde{p}}{\tilde{p}})^a(\frac{q_0}{1-q_0})^a\big), & \text{if } \ q_0 \in [0,\tilde{p}) \\ 0, & \text{if } \ q \in [\tilde{p},1] \end{cases}$$
$$\tilde{\alpha}(q) = M$$
$$C_3(q_0) = \begin{cases} q_0\, V_3(q_0) + l_f(1-q_0)(\frac{1-\tilde{p}}{\tilde{p}})^{a+1}(\frac{q_0}{1-q_0})^{a+1}, & \text{if } \ q_0 \in [0,\tilde{p}) \\ l_f(1-q_0), & \text{if } \ q_0 \in [\tilde{p},1] \end{cases}$$

(VII.58)
$$\bullet \text{ If } \tfrac{r\sigma^2}{M^2} < 1:$$
$$V_3(q_0) = \begin{cases} \frac{M}{r}\big(1 - (\frac{a+1}{2})(\frac{1-\tilde{q}^*}{\tilde{q}^*})^a(\frac{q_0}{1-q_0})^a\big), & \text{if } \ q_0 \in [0,\tilde{q}^*] \\ \frac{a^2 M}{r(1+2a)}(\frac{(1-\tilde{q}^*)q_0}{\tilde{q}^*(1-q_0)})^{a+1}\big((\frac{\tilde{p}(1-q_0)}{(1-\tilde{p})q_0})^{2a+1} - 1\big), & \text{if } \ q_0 \in (\tilde{q}^*,\tilde{p}) \\ 0, & \text{if } \ q \in [\tilde{p},1] \end{cases}$$
$$\tilde{\alpha}(q) = \begin{cases} M, & \text{if } \ q \in [0,\tilde{q}^*] \\ 0, & \text{if } \ q \in (\tilde{q}^*,1] \end{cases}$$
$$C_3(q_0) = \begin{cases} q_0\, V_3(q_0) + l_f(1-q_0)(\frac{1-\tilde{p}}{\tilde{p}})^{a+1}(\frac{q_0}{1-q_0})^{a+1}, & \text{if } \ q_0 \in [0,\tilde{p}) \\ l_f(1-q_0), & \text{if } \ q_0 \in [\tilde{p},1] \end{cases}$$

where the constant a is defined in (VII.14)*, $\tilde{p}$ is defined in* (VII.49)*, and*

(VII.59)
$$\tilde{q}^* := \frac{1}{1 + (\frac{1+a}{2a^2})^{\frac{1}{1+2a}}(\frac{1-\tilde{p}}{\tilde{p}})}.$$

Also, (III.5) *holds.*

PROOF:

We give the proof for the case $\frac{r\sigma^2}{M^2} \geq 1$ only. The case $\frac{r\sigma^2}{M^2} < 1$ can be done similarly. When $\frac{r\sigma^2}{M^2} \geq 1$, we observe that $a \geq 1$ and $\tilde{q}^* \in (0,\tilde{p}]$. One can check that V_3 in (VII.58) satisfies

(VII.60)
$$\begin{cases} V_3(0) = \frac{M}{r}, \\ M - rV_3(q) + \frac{q^2(1-q)^2M^2V_3''(q)}{2\sigma^2} + \frac{q(1-q)^2M^2V_3'(q)}{\sigma^2} = 0, & \text{if } \ q \in [0,\tilde{q}^*] \\ -rV_3(q) + \frac{q^2(1-q)^2M^2V_3''(q)}{2\sigma^2} - \frac{q^2(1-q)M^2V_3'(q)}{\sigma^2} = 0, & \text{if } \ q \in (\tilde{q}^*,\tilde{p}) \\ V_3(q) = 0, & \text{if } \ q \in [\tilde{p},1] \end{cases}$$

and $V_3 \in C^2([0,\tilde{p}))$. V_3 also satisfies following inequality:

$$\begin{cases} V_3'(q) + \frac{\sigma^2}{M(1-q)q} = \frac{\sigma^2}{M(1-q)q} \cdot \big(1 - (\frac{1-\tilde{q}^*}{\tilde{q}^*})^a (\frac{q}{1-q})^a\big) \geq 0, & q \in [0,\tilde{q}^*] \\ V_3'(q) + \frac{\sigma^2}{M(1-q)q} = -\frac{\sigma^2\big(1+2a-2a\big(\frac{(1-\tilde{q}^*)q}{\tilde{q}^*(1-q)}\big)^{a+1} - \big(\frac{(1-q)\tilde{q}^*}{q(1-\tilde{q}^*)}\big)^a\big)}{(1+2a)M(1-q)q} < 0, & q \in (q^*,\tilde{p}) \end{cases}$$

Then (VII.60) and the above inequalities imply

$$\begin{aligned} &- rV_3(q) - V_3'(q) \cdot \tfrac{q^2(1-q)M^2}{\sigma^2} + \tfrac{1}{2}V_3''(q) \cdot \tfrac{q^2(1-q)^2M^2}{\sigma^2} \\ &\qquad + \max_{\Delta\in[0,M]} \big(V_3'(q) \cdot \tfrac{q(1-q)M}{\sigma^2} + 1\big)\Delta = 0, \quad \text{for } q \in [0,\tilde{p}) \end{aligned} \tag{VII.61}$$

where the maximizing Δ is M for $q \in [0,\tilde{q}^*]$ and 0 for $q \in (\tilde{q}^*,\tilde{p})$. Using (VII.61) and following the procedure (VII.32)-(VII.35) in the current setup, we conclude that V_3 is the attacker's value function and $\tilde{\alpha}$ in (VII.58) is the optimal strategy, i.e., (VII.56) and the following equality hold:

$$V_3(q_0) = \max_{0\leq(\Delta_t)_{t\in[0,\infty)}\leq M} \mathbb{E}\Big[\int_0^{T\wedge\tau_{\tilde{p}}} \Delta_t dt \,\Big|\, \theta = 1\Big].$$

Now it remains to consider the defender's cost. We observe that the defender's expected cost can be rewritten as

$$\begin{aligned} &\mathbb{E}\Big[\Big(\int_0^{T\wedge\tau_{\tilde{p}}} \tilde{\alpha}(q_t)\,dt\Big) \cdot 1_{\{\theta=1\}} + l_f \cdot 1_{\{\theta=0,\,\tau_{\tilde{p}}<T\}}\Big] \\ &= V_3(q_0)\cdot q_0 + \mathbb{E}\big[l_f \cdot e^{-r\tau_{\tilde{p}}} \,\big|\, \theta = 0\big] \cdot (1-q_0). \end{aligned} \tag{VII.62}$$

Therefore, to prove that C_3 in (VII.58) is the corresponding defender's expected cost, it is enough to show that $U_0(q_0) = \mathbb{E}\big[e^{-r\tau_{\tilde{p}}} \,\big|\, \theta = 0\big]$ where

$$U_0(q) = \begin{cases} (\frac{1-\tilde{p}}{\tilde{p}})^{a+1}(\frac{q}{1-q})^{a+1}, & \text{if } \ q \in [0,\tilde{p}) \\ 1, & \text{if } \ q \in [\tilde{p},1] \end{cases} \tag{VII.63}$$

When $\theta = 0$, the Ito's formula and (VII.63) produce

$$e^{-r\tau_{\tilde{p}}} = e^{-r\tau_{\tilde{p}}}U_0(q_{\tau_{\tilde{p}}}) = U_0(q_0) + \int_0^{\tau_{\tilde{p}}} \tfrac{e^{-rt}q_t(1-q_t)M}{\sigma^2} U_0'(q_t) dW_t. \tag{VII.64}$$

Since the stochastic integral in (VII.64) is a square-integrable martingale, we obtain the desired result, $\mathbb{E}\big[e^{-r\tau_{\tilde{p}}} \,\big|\, \theta = 0\big] = U_0(q_0)$.

Finally, suitable use of LHospital's rule and $a = \mathcal{O}(\frac{1}{M^2})$ for large M produce (III.5).

Proof of Proposition III.3:

When M is large enough ($\frac{r\sigma^2}{M^2} < 1$), the expression of expected cost of the defender can be found in (VII.21). Using (VII.22), we rewrite the expected cost as

$$C_e(q_0) = \begin{cases} q_0\Big(\frac{M}{r} - \frac{\sigma^2}{a(a+1)M}\big(\frac{e^{b^2}M}{2rl_f}\big)^a\big(\frac{q_0}{1-q_0}\big)^a\Big), & \text{if } \ q_0 \in [0, q^*] \\ l_f(1-q_0)e^{-y(q_0)^2}, & \text{if } \ q_0 \in (q^*, p) \\ l_f(1-q_0), & \text{if } \ q_0 \in [p, 1] \end{cases} \tag{VII.65}$$

In (VII.14), we observe that for large M, $a = \mathcal{O}(\frac{1}{M^2})$ and $b = \mathcal{O}(M)$. This implies $\lim_{M\to\infty} c = 1$ and $\lim_{M\to\infty} p = \frac{l_f\sqrt{\pi r}}{l_f\sqrt{\pi r}+\sigma}$. Using this observation, we also conclude that $\lim_{M\to\infty} q^* = 0$. In (VII.65), $\lim_{M\to\infty} y(q_0) = 1 - \frac{\sigma q_0}{l_f\sqrt{\pi r}(1-q_0)}$ produces (III.7).

E. Proof of Propositions in Section IV

Proof of Proposition IV.1: (1) If $\frac{r\sigma^2}{M} \geq 1$, then obviously $p = \tilde{p}$. In case $\frac{r\sigma^2}{M} < 1$, we have $p = \frac{cl_f\sqrt{\pi r}}{cl_f\sqrt{\pi r}+\sigma}$ and $\tilde{p} = \frac{(1+a)rl_f}{(1+a)rl_f+aM}$. Then, $p \leq \tilde{p}$ is equivalent to $c \leq \frac{(1+a)\sigma\sqrt{r}}{aM\sqrt{\pi}}$. Using the relation (VII.14), we obtain $\frac{(1+a)\sigma\sqrt{r}}{aM\sqrt{\pi}} - c = \psi(b)$, where

$$\psi(b) := \tfrac{2(b+\sqrt{4+b^2})}{\sqrt{\pi}(2-b^2+b\sqrt{4+b^2})} - \varphi(b) - \tfrac{4e^{-b^2}}{\sqrt{\pi}(3b+\sqrt{4+b^2})}. \tag{VII.66}$$

Since $b > 0$ for $\frac{r\sigma^2}{M} < 1$, it remains to check that $\psi(b) \geq 0$ for $b > 0$. Observe that

$$\psi'(b) = \tfrac{16e^{-b^2}\left(2+2b^3-3b^5-b^7+(1-2b^2+b^4+b^6)\sqrt{4+b^2}+e^{b^2}(11b^3-b+(5b^2-1)\sqrt{4+b^2})\right)}{\sqrt{\pi}\sqrt{4+b^2}(3b+\sqrt{4+b^2})^2(2-b^2+b\sqrt{4+b^2})^2} \tag{VII.67}$$

$$= \tfrac{b^3(12+7b^2+10b^4)+b^2(2+5b^2+6b^4)\sqrt{4+b^2}+(e^{b^2}-1-b^2-b^4)(11b^3-b+(5b^2-1)\sqrt{4+b^2})}{\frac{1}{16}\sqrt{\pi}\sqrt{4+b^2}(3b+\sqrt{4+b^2})^2(2-b^2+b\sqrt{4+b^2})^2e^{b^2}} \tag{VII.68}$$

We check that $2 + 2b^3 - 3b^5 - b^7 + (1 - 2b^2 + b^4 + b^6)\sqrt{4+b^2} \geq 0$ since $(1 - 2b^2 + b^4 + b^6)^2(4 + 2b^2) - (2 + 2b^3 - 3b^5 - b^7)^2 = 4(1 - 2b)^2 \geq 0$. Therefore, if $11b^3 - b + (5b^2 - 1)\sqrt{4+b^2} \geq 0$, then (VII.67) implies $\psi'(b) \geq 0$. In case $11b^3 - b + (5b^2 - 1)\sqrt{4+b^2} < 0$, then we should have $b < 1$ and $e^{b^2} \leq 1 + b^2 + b^4$, and (VII.68) implies $\psi'(b) \geq 0$.

In summary, $\psi'(b) \geq 0$ for $b > 0$. Since $\psi(0) = 0$, we conclude that $\psi(b) \geq 0$ for $b > 0$.

(2) We prove that p is a decreasing function of M. Other cases can be proved similarly. In case $\frac{r\sigma^2}{M} \geq 1$, we have $p = \frac{(1+a)rl_f}{(1+a)rl_f+aM}$. We substitute a in (VII.14)

to the expression of p and compute the derivative:

$$\frac{\partial p}{\partial M} = -\frac{8l_f r^2\sigma^2(\sqrt{M^2+8r\sigma^2}-2M)}{\sqrt{M^2+8r\sigma^2}\big(-M^2+l_f r\sqrt{M^2+8r\sigma^2}+M(l_f r+\sqrt{M^2+8r\sigma^2})\big)^2} < 0, \quad \text{because } \frac{r\sigma^2}{M} \geq 1.$$

In case $\frac{r\sigma^2}{M} < 1$, we have $p = \frac{cl_f\sqrt{\pi r}}{cl_f\sqrt{\pi r}+\sigma}$. We substitute c in (VII.14) to the expression of p and compute the derivative:

$$\frac{\partial p}{\partial M} = -\frac{e^{-b^2}l_f\big(\sqrt{(M^3+6Mr\sigma^2)^2+32r^3\sigma^6}-M^3-6Mr\sigma^2\big)}{M^2\sqrt{M^2+8r\sigma^2}(\sigma+l_f\sqrt{\pi r}c)^2} < 0.$$

Proof of Proposition IV.1: In Theorem VII.3, it is already proved that α in Proposition VII.2 is the optimal attack-intensity. Then the form of α immediately implies the proposition.

Proof of Proposition IV.1: (1) Using the expression (VII.20), we obtain $\lambda'(p) = -\frac{4p\sqrt{r}}{c\sigma\sqrt{\pi}} < 0$.

(2) In case $\frac{r\sigma^2}{M} \geq 1$, $\lambda(q)$ does not depend on l. In case $\frac{r\sigma^2}{M} < 1$, using the expression (VII.20), we obtain

$$\frac{\partial}{dl}\big(\lambda(q)\big) = \begin{cases} 0, & \text{if } \ q \in [0, q^*] \\ \frac{2a(1+a)Mr\sqrt{r}(1-q)^2\big(e^{-y(q)^2}-c\sqrt{\pi}(\frac{(1-p)q}{p(1-q)})y(q)\big)}{c(1-p)^2\sigma\sqrt{\pi}(aM+(1+a)rl_f)^2}, & \text{if } \ q \in (q^*, p) \\ 0, & \text{if } \ q \in [p, 1] \end{cases}$$

where $y(x)$ is defined in (VII.14). To check $\frac{\partial}{dl}\big(\lambda(q)\big) \geq 0$, it is enough to show that $e^{-y(x)^2} - c\sqrt{\pi}(\frac{(1-p)x}{p(1-x)})y(x) \geq 0$ for $q \in (q^*, p)$. Indeed,

$$\begin{aligned} &(e^{-y(q)^2} - c\sqrt{\pi}(\tfrac{(1-p)q}{p(1-q)})y(q))\big|_{q=q^*} = ae^{-b^2} > 0, \\ &\frac{d}{dq}\big(e^{-y(q)^2} - c\sqrt{\pi}(\tfrac{(1-p)q}{p(1-q)})y(q)\big) = \tfrac{c^2\pi q(1-p)^2e^{y(q)^2}}{2p^2(1-q)^3} > 0, \end{aligned}$$

and we obtain the desired result.

F. Proof of Propositions in Section V

Proof of Proposition V.1: We first prove the following lemma.

LEMMA VII.6: *Let $(q_t)_{t\geq 0}$ be the defender's equilibrium belief process in* (II.1)*. Then, q_t never hit* 0 *almost surely, i.e.,*

$$\mathbb{P}(\tau_0 = \infty) = 0, \quad \textit{where} \quad \tau_0 := \inf\{t \geq 0 : q_t = 0\}. \tag{VII.69}$$

PROOF:

By the 1-dimensional comparison result (see Proposition 5.2.18 in Karatzas and Shreve (1998)), it is enough to show (VII.69) condition on $\theta = 0$. When $\theta = 0$, q_t satisfies the following SDE:

$$dq_t = -\frac{q_t^2(1-q_t)\alpha(q_t)^2}{\sigma^2}dt + \frac{q_t(1-q_t)\alpha(q_t)}{\sigma}dW_t. \tag{VII.70}$$

We apply the Feller's Test for explosions using the *scale function* and *speed measure* (for details, see Chapter 5.5(C) in Karatzas and Shreve (1998)). Let $x_0 \in (0,p)$ be a fixed number. The scale function s of (VII.70) is defined as

$$\begin{aligned} s(x) &:= \int_{x_0}^{x} \exp\Big(-2\int_{x_0}^{z} \frac{-\frac{\zeta^2(1-\zeta)\alpha(\zeta)^2}{\sigma^2}}{(\frac{\zeta(1-\zeta)\alpha(\zeta)}{\sigma})^2}d\zeta\Big)dz \\ &= \tfrac{(1-x_0)^2}{1-x} - (1-x_0) \end{aligned} \tag{VII.71}$$

Then the corresponding speed measure m on $(0,p)$ is

$$m(dz) := \frac{dz}{s'(z)(\frac{z(1-z)\alpha(z)}{\sigma})^2} = \frac{\sigma^2}{(1-x_0)^2 z^2 \alpha(z)^2}\,dz \tag{VII.72}$$

According to the proof in Theorem 5.5.29 in Karatzas and Shreve (1998), to show (VII.69), it is enough to show that

$$\lim_{x\downarrow 0}\int_{x_0}^{x}(s(x)-s(z))m(dz) = \infty. \tag{VII.73}$$

Indeed, if x_0 is chosen small enough, then $\alpha(z) = M$ for $z \le x_0$, and

$$\int_{x_0}^{x}(s(x)-s(z))m(dz) = \frac{\sigma^2}{M^2}\int_{x_0}^{x}\Big(\frac{1}{1-x}-\frac{1}{1-z}\Big)\cdot\frac{1}{z^2}\,dz \to \infty,$$

as $x \downarrow 0$. Therefore (VII.73) holds and the proof is done.

Now we prove (V.1). Recall that $(q_t)_{t\ge 0}$ is a martingale under the filtration $(\mathcal{F}_t^Y)_{t\in[0,\infty)}$. For $0 < q_0 < p$, consider $0 < \epsilon < q_0$ and $\tau_\epsilon := \inf\{t \ge 0 : q_t = \epsilon\}$. Then, by the optional sampling theorem, we have

$$q_0 = \mathbb{E}[q_{\tau_p \wedge \tau_\epsilon}] = \epsilon\ \mathbb{P}(\tau_\epsilon < \tau_p) + p\ \mathbb{P}(\tau_p < \tau_\epsilon).$$

The above equality produces

$$\mathbb{P}(\tau_p < \tau_\epsilon) = \frac{q_0 - \epsilon}{p - \epsilon}. \tag{VII.74}$$

$\lim_{\epsilon\downarrow 0}\tau_\epsilon = \tau_0$, Lemma VII.6 and (VII.74) implies (V.1).

Proof of Proposition V.2: We first obtain the form of the equilibrium in the following theorem.

THEOREM VII.7: *Assume that $l_s < r\ l_f$. Then there exists an equilibrium in Definition II.1 with the defender's cost minimization problem* (V.2).

PROOF:
If $\frac{r\sigma^2}{M^2} \geq 1$, we define p and U as

$$U(q) = \begin{cases} \frac{l_s}{r} + q\Big(\frac{M}{r} - \big(\frac{l_s+M}{a(1+r)}\big)\big(\frac{1-p}{p}\big)^a\big(\frac{q}{1-q}\big)^a\Big), & \text{if } \ q \in [0,p) \\ (1-q)l_f, & \text{if } \ q \in [p,1] \end{cases}$$
$$p = \frac{(1+a)(r\,l_f - l_s)}{(1+a)(r\,l_f - l_s) + a(M+l_s)},$$

and if $\frac{r\sigma^2}{M^2} < 1$, we define p and U as

$$U(q) = \begin{cases} \frac{l_s}{r} + q\Big(\frac{M}{r} - M\big(\frac{1}{2r} + \frac{a\,l_s}{c\sqrt{\pi}r^{\frac{3}{2}}\sigma}\big)\big(\frac{1-q^*}{q^*}\big)^a\big(\frac{q}{1-q}\big)^a\Big), & \text{if } \ q \in [0,q^*] \\ \frac{l_s}{r} + \frac{\sigma\,q\,y(q)}{\sqrt{r}} + \frac{((1-p)rl_f - l_s)\Big(p(1-q)e^{-y(q)^2} - c\sqrt{\pi}(1-p)q\,y(q)\Big)}{(1-p)pr}, & \text{if } \ q \in (q^*,p) \\ (1-q)l_f, & \text{if } \ q \in [p,1] \end{cases}$$
$$p = \frac{c\sqrt{\pi r}(l_f - \frac{l_s}{r})}{c\sqrt{\pi r}(l_f - \frac{l_s}{r}) + \sigma + \frac{l_s(c^2\pi - 2)}{c\sqrt{\pi r}}}.$$

Let V and α as (VII.15), (VII.16), (VII.19) and (VII.20) with p defined above. Trivial modification of the proof of Theorem VII.3 shows that p is the equilibrium threshold, U is the defender's expected cost, V is the attacker's expected profit, and α is the attack-intensity.

Then, the expression of U, the defender's expected cost, in Theorem VII.7 implies the result in Proposition V.2.

REFERENCES

Anderson, Axel and Lones Smith, "Dynamic deception," *The American Economic Review*, 2013, *103* (7), 2811–2847.

Aumann, Robert J and M Maschler, "Game theoretic aspects of gradual disarmament," *Report of the US Arms Control and Disarmament Agency*, 1966, *80*, 1–55.

Back, Kerry and Shmuel Baruch, "Information in securities markets: Kyle meets Glosten and Milgrom," *Econometrica*, 2004, *72* (2), 433–465.

Chen, Chia-Mei and Hsiao-Chung Lin, "Detecting botnet by anomalous traffic," *Journal of Information Security and Applications*, 2015, *21*, 42 – 51.

Crawford, Vincent P, "Lying for strategic advantage: Rational and boundedly rational misrepresentation of intentions," *The American economic review*, 2003, *93* (1), 133–149.

He, Shu, Gene Moo Lee, Sukjin Han, and Andrew B Whinston, "How would information disclosure influence organizations outbound spam volume? Evidence from a field experiment," *Journal of Cybersecurity*, 2016, *2* (1), 99–118.

Hendricks, Kenneth and R Preston McAfee, "Feints," *Journal of Economics & Management Strategy*, 2006, *15* (2), 431–456.

Kyle, Albert S, "Continuous auctions and insider trading," *Econometrica: Journal of the Econometric Society*, 1985, pp. 1315–1335.

Liptser, Robert and Albert Shiryaev, *Statistics of Random Processes*, Springer, 2001.

Wald, Abraham, "Sequential tests of statistical hypotheses," *The Annals of Mathematical Statistics*, 1945, *16* (2), 117–186.

Wald, ABRAHAM and J Wolfowitz, "Bayes solutions of sequential decision problems," *Proceedings of the National Academy of Sciences*, 1949, *35* (2), 99–102.