Towards Systemic Risk Evaluation, Attribution, and Mitigation in Networked Systems: Work in Progress

Vladimir Marbukh[1] and Michael Marbukh[2]

[1] National Institute of Standards and Technology, Gaithersburg MD 20899, USA
[2] Independent researcher, New Market MD 21774, USA
marbukh@nist.gov

Abstract. Conventional game-theoretic models of systemic risk evaluation and mitigation in networks with selfish components are based on classical economics which assumes risk neutral/averse decision makers. While the corresponding game-theoretic models have unique Nash equilibrium, our analysis of the Susceptible-Infected-Susceptible (SIS) contagion under behavioral economic model for selfish components, indicates a possibility of multiple Nash equilibria. This possibility has important practical implications, e.g., "unacceptably" high Price of Anarchy (PoA) associated with "non-efficient" Nash equilibria may warrant additional mechanism for the purpose of avoidance of inefficient Nash equilibria. Infeasibility of centralized control of dynamic processes in large-scale networks motivates interest in decentralized strategies. However, decentralized mitigation of the systemic risk, which is inherently a collective phenomenon, requires some level of global view by individual network components. On an example of SIS contagion, we suggest that this global view can be provided with few system-wide "macro-parameters." Finally, we report our initial results on microeconomic modeling of cyber security investments.

Keywords: Systemic risk evaluation, attribution and mitigation, Behavioral Economics, Entropic Value at Risk, cybersecurity microeconomic model, Gordon-Loeb model.

1 Introduction

Numerous systemic failures of various large-scale networked systems [1] demonstrate multifaceted challenges of systemic risks evaluation, attribution, and mitigation. These challenges are due to tensions between economic incentives of different system components as well as between economic efficiency driving system towards the boundary of the operational region and desire to maintain the "safety margin." Also, inherently collective nature of systemic events makes decentralized evaluation and mitigation of the systemic risk by individual components of a large-scale networked system practically infeasible. This paper discusses and proposes approaches to addressing some of these challenges.

Section 2 considers implications of the central assumption of Behavioral Economics (BE) that system components may be risk seeking [2]. Following conventional

approach, the system is modelled as a non-cooperative game of different network components, where system equilibrium is associated with the Nash equilibria [3]. Typically, this analysis is based on the classical economics with risk neutral and risk averse system components characterized by linear and, respectively, concave utilities [3]. Although some aspects of BE on systemic risk have been analyzed, e.g., in [4], implications of the central BE assumption that some decision makers may be risk seeking [2], have not received proper attention. While for risk neutral/averse system components, the corresponding game typically has a unique Nash equilibrium [3], our analysis of selfish Susceptible-Infected-Susceptible (SIS) infection risk mitigation under BE model indicates a possibility of multiple Nash equilibria. This possibility has important practical implications, e.g., "unacceptably" high Price of Anarchy (PoA) associated with "non-efficient" Nash equilibria may warrant additional mechanism for the purpose of avoidance of the highly inefficient Nash equilibria.

Section 3 suggests a possibility of evaluation and subsequent mitigation of the individual systemic risk with limited global information provided by a central trusted authority. While we consider a case of SIS contagion and Entropic Values at Systemic Risk (EVaSR) [5] for individual network nodes, our analysis is applicable to other systemic events analogous to continuous and discontinuous phase transitions [6]. Due to similarity of SIS contagion with continuous phase transitions, we use Landau theory of phase transitions to evaluate EVaSR for individual nodes under large deviation regime [6]-[8]. We propose this systemic risk attribution to individual network nodes, where each node's share is determined by a combination of local to the node "microparameters," and a small number of network-wide "macro-parameters". Assuming that these macro-parameters are communicated to individual nodes by some trusted entity, e.g., government, individual nodes combine the corresponding global and locally available information to manage the individual systemic risks. Future work should verify these assertions by theoretical analysis and simulations, as well as determine their practical implications.

Finally, section 4 reports on work in progress on microeconomic modeling of cyber security investments for a "generalized monotonic structures." Highly aggregated macroeconomic Gordon-Loeb (G-L) optimization model for cyber security investments [9] assumes known system-level security risk reduction return on investment measured by the corresponding macroeconomic marginal utility. However, derivation of this macroeconomic marginal utility from the system-specific microeconomic model for cybersecurity investments remains a missing link in analysis of specific systems. Section 4 outlines an approach to bridging this gap by generalizing model [10] with multiplicative residual risk.

2 Systemic Risk under Prospect Theory

Consider a SIS model on a connected graph with N nodes, where each node is either "healthy" or "infected". Once node $i = 1,..,N$ becomes infected, it spreads infection to each of its neighboring nodes j at fixed rate $\lambda > 0$. Node i recovery rate is $\mu_i = \mu_{i0} c_i$, where $c_i \geq 0$ is this node's investment in its recovery capability. Node i gross

utility is $L_i u_i(1-\pi_i)$, where L_i is loss rate experienced by infected node i, this node normalized gross utility $u_i(1-\pi_i)$ increases from $u_i(0)=0$ to $u_i(1)=1$, and node i persistent infection probability is $\pi_i \in [0,1]$. Since probability π_i is a function of node i investment c_i as well as vector of investments by other nodes $c_{-i}=(c_j, j\neq i)$: $\pi_i = \pi_i(c_i, c_{-i})$, each node gross utility is a function of investments by all nodes in the network: $U_i(c_i, c_{-i}) := L_i u_i[1-\pi_i(c_i, c_{-i})]$. Thus node $i=1,..,N$ maximization their net utilities $U_i(c_i, c_{-i}) - c_i$ over $c_i \geq 0$ can be naturally modeled as a non-cooperative game.

Fig. 1 demonstrates relation between attitude towards risk and shape of the utility function.

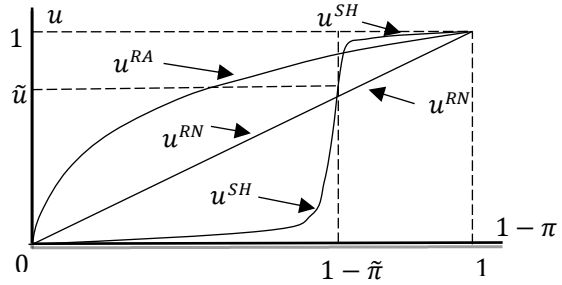


Fig. 1. Utilities of agents with different attitude towards risk.

Linear utility function u^{RN} represents risk neutral agents and concave function u^{RA} represents risk averse agents. Prospect theory [2] postulates S-shape utility function u^{SH}, which models agents who are risk averse for $\pi < \tilde{\pi}$ and risk seeking for $\pi > \tilde{\pi}$. Here reference, i.e., inflexion, point $\pi = \tilde{\pi}$ is agent specific. In addition to this, main assumption (A1), prospect theory postulates (A2): that users are more sensitive to losses than gains, i.e., $\tilde{u} > 1/2$, and (A3): that users overestimate low while underestimating high probabilities. While effect of assumptions (A2-3) has received some attention, e.g., in [4], implications of main assumption (A1) remain unclear. To highlight these implications, we assume a threshold-based utility function

$$u^{TH}(1-\pi|\tilde{\pi}) = \begin{cases} 0 & if \quad \pi > \tilde{\pi} \\ 1 & if \quad \pi < \tilde{\pi}, \end{cases} \tag{1}$$

which is an extreme case of S-shape utility function u^{SH}.

For simplicity we consider a regular network where all nodes $i=1,..,N$ have the same degrees $d_i = d \geq 1$, the same recovery rates $\mu_j = \mu = \mu_0 c$, $j=1,..,N$, the same gross utility functions $u_i(1-\pi_i) = u(1-\pi)$, the same investment levels $c_j = c$, and thus the same persistent infection probabilities $\pi_j(c) = \pi(c)$. It is known [3] that under mean-field approximation, $\pi(c)$ is given by the following expression:

$$\pi(c) := [1-(\mu_0 c)/(d\lambda)]^+, \tag{2}$$

where $[a]^+ := \max(0, a)$. Probabilities (2) represent a Nash equilibrium for the corresponding game if and only if no node has incentive to unilaterally deviate from this equilibrium. If node i invests $c_i = x$ while each other node $j \neq i$ invests $c_j = c$, then under mean-field approximation node i infection probability is

$$\pi_i = \pi(x, c) := \frac{d\lambda\pi(c)}{d\lambda\pi(c)+\mu_0 x}, \tag{3}$$

and thus node i gross utility is $U(x,c) := Lu^{TH}[1-\pi(x,c)]$, where $u^{TH}(.)$ is a threshold-based utility (1). It is easy to verify that

$$U(x,c) = \begin{cases} 0 & if \quad x \le \tilde{x}(c) \\ L & if \quad x > \tilde{x}(c) \end{cases}, \tag{4}$$

where $\tilde{x}(c) = (1/\tilde{\pi} - 1)[d\lambda/\mu_0 - c]^+$.

Fig. 2 plots utility (4) as a function of x for different c.

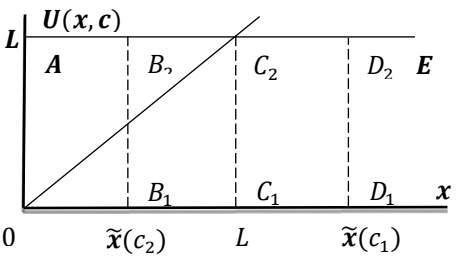


Fig. 2. Threshold-based utility vs. investment.

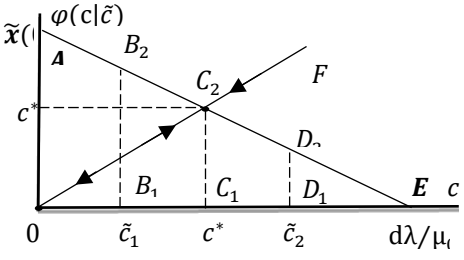


Fig. 3. Solution to equation (6)-(7).

In Fig. 2, $0 \le c_1 < \tilde{c} < c_2 < d\lambda/\mu_0$, where $\tilde{c} = d\lambda/\mu_0 - L\tilde{\pi}/(1-\tilde{\pi})$. For $c \ge d\lambda/\mu_0$, utility $U(x,c)$ follows line AE since $\tilde{x}(c) = 0$.

Given $c \ge 0$, each node determines investment amount $\varphi(c)$ by maximizing its net utility:

$$\varphi(c) := arg \max_{x \ge 0}\{U(x,c) - x\}. \tag{5}$$

Nash equilibria of the corresponding game naturally can be associated with asymptotically stable solutions of the following fixed-point equation [11]:

$$c = \varphi(c), \tag{6}$$

where, as it is easy to verify that

$$\varphi(c) = \begin{cases} 0 & if \quad c \le \tilde{c} \\ \tilde{x}(c) & if \quad c > \tilde{c} \end{cases}, \tag{7}$$

and $\tilde{c} = d\lambda/\mu_0 - L\tilde{\pi}/(1-\tilde{\pi})$.

Fig. 3 shows solution to fixed-point equation (6)-(7) for different $\tilde{c} = 0 < \tilde{c}_1 < c^* < \tilde{c}_2 < L$, where

$$c^* = (1-\tilde{\pi})(d\lambda/\mu_0). \tag{8}$$

If $\tilde{c} \le 0$ or $\tilde{c} > c^*$, equation (6)-(7) has unique stable solution $c = c^*$ or $c = 0$ respectively. If $1 - \tilde{\pi} < L\,\mu_0/(d\lambda) < (1-\tilde{\pi})/\tilde{\pi},\ 0 < \tilde{c} < c^*$, these two solutions coexist as locally stable.

Following conventional interpretation [11], we associate locally stable solutions of fixed-point equation (6)-(7) with equilibrium investment levels. Analysis suggests that while equilibrium $c = c^*$ is reminiscent of competitive equilibrium in a case of risk neutral/averse nodes, equilibrium $c = 0$ is a result of S-shape of the node utilities. Existence of a broad range of system parameters when two metastable equilibria coexist if $\tilde{\pi} << 1$ is a result of high cost of a unilateral "gainful" deviation from highly inefficient with respect to the corresponding Price of Anarchy equilibrium $c = 0$. While these qualitative assertions can be easily quantified within this paper's homogeneous model, currently we are investigating a possibility and implications of multiple equilibria in heterogeneous networks, using approach [7]. Probably, the most important

implication of such a possibility is necessity of a mechanism preventing system from remaining in an inefficient equilibrium for an "extended time period."

3 Towards Systemic Risk Attribution

Figure 4 depicts average portion of infected nodes π in a SIS contagion as a function of the "effective" infection rate ρ. From the perspective of phase transitions, portion π plays role of the order parameter, and rate ρ plays role of exogenous parameter: $\pi = 0$ for $\rho \leq \rho^*$ and $\pi > 0$ for $\rho > \rho^*$. Due to similarity of SIS contagion with continuous phase transitions, we use Landau theory of phase transitions to evaluate Entropic Value at Systemic Risk (EVaSRs) for individual nodes under large deviation regime [6]-[7], [12].

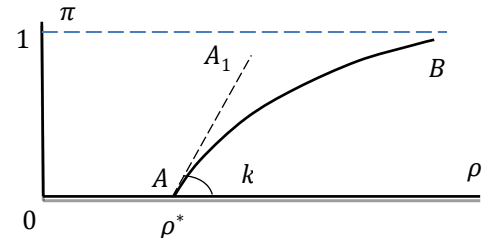


Fig. 4. Portion of infected nodes vs. effective infection rate.

We demonstrate that these individual EVaSRs are determined by a combination of local to the node "microparameters," and a small number of network-wide "macro-parameters": margin $\rho^* - \rho$ and slope k just beyond the transition point ρ^* (see Fig 4). Then system components combine this global information, provided by some trusted entity, e.g., government, with locally available information to manage the individual systemic risks. Future work should verify these assertions by theoretical analysis and simulations, as well as determine their practical implications. The proposed analysis is able to quantify tension between higher infection threshold $\rho = \rho^*$ and higher losses, represented by slope k, if this threshold is breached [12]-[13]. This tension may result in abrupt/discontinuous systemic failures, which carry higher risk than gradual/continuous systemic events due to possible metastability [8].

Consider a SIS model on a connected graph with N nodes and with adjacency matrix $A = (A_{ij})_{i,j=1}^{N}$, where each node is either "healthy" or "infected". Once node $i = 1,..,N$ becomes infected, it spreads infection to each of its neighboring nodes j at fixed rate $\lambda > 0$. Node i recovery rate is $\mu_i = \mu_{i0} c_i$, where $c_i \geq 0$ is this node investment in its recovery capability. Under these assumptions, vector $\delta(t) = (\delta_i(t), i = 1,..,N)$ is a controlled Markov process with 2^N states $\delta \in \{0,1\}^N$ and continuous time $t \geq 0$. To avoid infection-free state $\delta = 0$ to be absorbing state regardless of system parameters, we assume that each node $i = 1,..,N$ can be "self-infected" with rate $\varepsilon\lambda$, where small parameter $\varepsilon \ll 1$. Due to very high dimension 2^N of the corresponding Kolmogorov system, we consider mean-field approximation for steady-state probabilities of nodes being infected at moment t, $p_i = P\{\delta_i(t) = 1\}$ [3]:

$$p_i = \frac{\lambda(\varepsilon+\sum_{j\neq i}A_{ij}p_j)}{\mu_{i0}c_i+\lambda(\varepsilon+\sum_{j\neq i}A_{ij}p_j)}. \quad (9)$$

Further we disregard terms of order $O(\varepsilon)$ as $\varepsilon \downarrow 0$.

Let $\alpha = (\alpha_1,..,\alpha_N)$ and $\beta = (\beta_1,..,\beta_N)$ be the left and right eigenvectors of matrix $B(c) = (A_{ij}/(\mu_{i0}c_i))_{i,j=1}^N$, associated with Perron-Frobenius eigenvalue γ, and normalized as follows: $\alpha\beta^T = 1$. It is known that system (9) always has unique solution $p^* = (p_1^*,\dots,p_N^*)$: $p^* = o(\varepsilon)$ if $\lambda \leq \lambda^* := 1/\gamma$, and $p^* = O(1)$ if $\lambda > \lambda^*$ as $\varepsilon \downarrow 0$. It can be shown [12], [14] that

$$p_i^* = \frac{\alpha_i}{\sum_j \alpha_j^2\beta_j}(1-\lambda_*/\lambda) + o(1-\lambda_*/\lambda) \text{ as } \lambda \downarrow \lambda^*. \quad (10)$$

For an undirected uncorrelated network, infection threshold is

$$\lambda^* = d_{ave}/\langle d^2\tau_d\rangle = d_{ave}/\langle d^2/(\mu_{d0}c_d)\rangle, \quad (11)$$

where the average node degree d_{ave} and averages $\langle . \rangle$ are evaluated over node degree distribution. It is also known that infection probability for a node of degree d at the onset of systemic infection is

$$p_d^* = (1/b)(1-\lambda_*/\lambda)[d/(\mu_{d0}c_d)] \text{ as } \lambda \downarrow \lambda_* \quad (12)$$

where $b = 2\langle d^3/(\mu_{d0}c_d)^2\rangle/d_{ave}$.

Infected node $i = 1,..,N$ suffers loss rate $h_i \geq 0$ and, being risk averse, mitigates its EVaR [5]

$$EVaSR_{i,1-\alpha} = h_i \, max_{P:KL(P\|P^*)\leq -\ln\alpha} E_P[\delta_i], \quad (13)$$

where the Kulback-Leibler (KL) deviation is

$$KL(P\|P^*) := \sum_\eta P(\delta) ln[P(\delta)/P^*(\delta)]. \quad (14)$$

Risk metric (13)-(14) represents the maximum expected node i loss with respect to all feasible distributions $P(\delta)$ subject to a given KL deviation from steady-state distribution $P^*(\delta)$. Here parameter $0 \leq 1-\alpha \leq 1$ characterizes decision maker risk averseness, and thus parameter α characterizes node risk tolerance. Node $i = 1,..,N$ loss is $L_i(c_i, c_{-i}) = EVaSR_{i,1-\alpha}(c_i, c_{-i}) + c_i$, where c_{-i}: $(c_j, j \neq i)$. Socially optimal risk mitigation minimizes the aggregate loss

$$c^{opt} = argmin_{c\geq 0} \sum_{i=1}^N [EVaSR_{i,1-\alpha}(c_i, c_{-i}) + c_i]. \quad (15)$$

Selfish risk mitigation can be associated with Nash equilibrium in a non-cooperative game $c^* = (c_i^*)$ where each agent $i = 1,..,N$ attempts to minimize this agent's individual loss:

$$c_i^* = argmin_{c_i\geq 0}[EVaSR_{i,1-\alpha}(c_i, c_{-i}^*) + c_i]. \quad (16)$$

Consider onset of SIS systemic congestion: $\lambda \approx \lambda_*$ under assumptions of Landau theory of continuous phase transitions [6]-[7]. We identify the instantaneous portion of infected nodes $\eta = N^{-1}\sum_{i=1}^N \delta_i$ with order parameter since $\eta = 0$ ($\eta > 0$) indicates absence (presence) of systemic contagion as $N \to \infty$. It is known [6], that at the onset of a continuous phase transition, due to critical slowdown, order parameter $\eta(t)$ evolves on a much slower time scale than the rest of dynamic variables in $\delta(t)$, given $\eta(t) = \eta$. This allows us to approximate the evolution of order parameter $\eta(t)$ by a Markov birth-death process $\tilde{\eta}(t) \in \{i/N : i = 0,1,\dots,N\}$, where process $\tilde{\eta}(t)$ transition rate from state $\eta = i/N$ to the neighboring states $(i-1)/N$ and $(i+1)/N$ can be explicitly evaluated [7]. It can be shown [7] that due to this separation of time scales,

$$EVaSR_{i,1-\alpha} \approx h_i E_P[\delta_i|\eta] \, max_{P:KL(P(\eta)\|P^*(\eta)\leq -\ln\alpha} E_P[\eta], \quad (17)$$

where in large deviation regime: $N \to \infty$, $\alpha_i \to 0$, $\tau_i := -N^{-1} ln\alpha_i = O(1)$ at the onset of the epidemic $\lambda \approx \lambda_*$, density

$$p^*(\eta;\lambda) = \begin{cases} Z^{-1}(\lambda) exp[-Nu(\eta;\lambda)] & if \quad 0 \le \eta \le 1 \\ 0 & otherwise \end{cases}, \tag{18}$$

and $Z(\lambda)$ is the normalization constant. Following [6], [12], consider approximation $u(\eta;\lambda) \approx \tilde{u}(\eta;\lambda)$, where

$$u(\eta) \approx \tilde{u}(\eta) = \begin{cases} [\eta - k(\lambda\gamma - 1)]^2/2 & if \quad 0 \le \eta \le 1 \\ \infty & otherwise \end{cases} \tag{19}$$

Potential (19) is depicted in Figure 5 for $\lambda_1 < \gamma^{-1} < \lambda_2$.

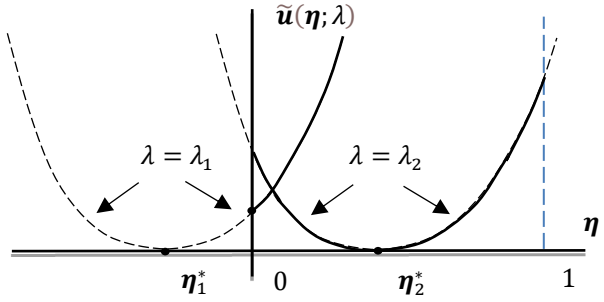


Fig. 5. Approximate effective potential (19): $\eta_i = k(\lambda\gamma - 1)$.

Combination of (17)-(19) suggest the following approximation for the individual risks.
Conjecture. Individual EVaSR (13)-(14) under (17)-(19) are:

$$EVaR_{i,1-\alpha} \approx \frac{\lambda d_i h_i}{\mu_{i0} c_i} \left[k(\lambda\gamma - 1) + \sqrt{2\tau_i}\right]^+, \tag{20}$$

where $[x]^+ := \max(0, x)$ ■
Approximation (20) states that individual risk, in addition to the local parameters, depends on the global parameters $\lambda^* = 1/\gamma$ and k, which, in turn, depend on the node investments $c_j, j = 1,..,N$.

This observation suggests the following iterative solutions to socially optimal and selfish optimizations (15) and (16) as follows:

$$c^{opt}(\lambda^*, k) = arg \min_{c \ge 0} \sum_{i=1}^{N} \left[EVaSR_{i,1-\alpha}(c_i|\lambda^*, k) + c_i\right], \tag{21}$$

and respectively

$$c_i^*(|\lambda^*, k) = arg \min_{c_i \ge 0} \left[EVaSR_{i,1-\alpha}(c_i|\lambda^*, k) + c_i\right]. \tag{22}$$

Assumption that some trusted centralized "agency" can evaluate global parameters λ^* and k, and then feed them back into optimizations (21)-(22), naturally leads to an intriguing possibility of a semi-distributed optimization. Issues of the convergence and the corresponding Price of Anarchy (PoA) are subjects of our current efforts.

4 Towards Risk Mitigation

Consider system with set of N potential vulnerabilities $\boldsymbol{V} = (v_n, n = 1,..,N)$ which can be exploited by adversaries. We identify set of exploited vulnerabilities with binary

vector $\delta = (\delta_1, .., \delta_N)$, where $\delta_n = 1$ if vulnerability v_n is exploited, and $\delta_n = 0$ otherwise. Exploits $\delta = (\delta_1, .., \delta_N)$ cause *economic loss* for the system $L(\delta)$, which satisfies certain natural assumptions [15]. We assume that system can reduce its exposure to potential vulnerabilities by employing strategy $T(\xi)$, $\xi \in \{0,1\}^N$, which eliminates vulnerability v_n if $\xi_n = 0$, and does not affect this vulnerability at all if $\xi_n = 1$, $n = 1, .., N$. Thus strategy $T(\xi)$ reduces the set of the feasible binary vectors δ to $\Delta_\xi := \{\delta: \delta \leq \xi, \delta \in \{0,1\}^N\}$, where we follow component-wise convention for vector inequality. We also assume that cost to the system of implementing strategy $T(\xi)$ is

$$C_\xi = \sum_{n=1}^N (1 - \xi_n) c_n, \tag{23}$$

i.e., cost of eliminating a set of potential vulnerabilities is additive with known costs of eliminating individual vulnerabilities v_n, c_n. In response to system strategy $T(\xi)$, attacker(s) employs a mixed strategy $A(Q_\xi)$, which is determined by probability distribution $Q_\xi(\delta)$ on Δ_ξ. Strategy $A(Q_\xi)$ exploits a subset of the set of remaining potential vulnerabilities v_n for all n such that $\delta_n = 1$ with probability $Q_\xi(\delta)$, $\delta \in \Delta_\xi$. We further assume that given attacker(s) strategy response to system lack of mitigation: $\xi = 1^N$, $Q(\delta) := Q_{1^N}(\delta)$, attacker(s) response to mitigation strategy $T(\xi)$, $\forall \xi \in \{0,1\}^N$ is $A(Q_\xi)$, where $Q_\xi(\delta) = Q(\delta | \delta \leq \xi)$ is the corresponding conditional distribution. Generalization to an arbitrary distribution $Q_\xi(\delta)$ on Δ_ξ is straightforward.

We quantify the residual, i.e., mitigated by employing strategy $T(\xi)$, system risk by the corresponding conditional expected system loss: $\bar{L}_\xi := E_{Q_\xi}[L(\delta)]$. Given security budget z, the optimal system strategy $T^*(z) = T[\xi^*(z)]$ minimizes the residual risk, given the aggregate cybersecurity budget z:

$$S(z) = min_{\xi \in \{0,1\}^N} \left\{ E_{Q_\xi}[L(\delta)] : \sum_{n=1}^N (1 - \xi_n) c_n \leq z \right\}. \tag{24}$$

The optimal aggregate cybersecurity budget $z = z^{opt}$ minimizes the total expected cost to the system:

$$z^{opt} = argmin_{z \geq 0} [\, S(z) + z], \tag{25}$$

which is a G-L model for optimal security investment [9].

In the rest of this paper, we illustrate optimization framework (24)-(25) on an example of a system with N potential vulnerabilities, where one or more exploited vulnerabilities cause system failure. Loss function for this system is

$$L(\delta) = L[1 - \prod_{n=1}^N (1 - \delta_n)], \tag{26}$$

and thus residual risk is

$$\bar{L}_\xi = L\left[1 - \prod_{n:\xi_n = 1} (1 - \rho_n)\right]. \tag{27}$$

We assume mutually independent probabilities of different exploits, probability of vulnerability v_n exploit $\rho_n = E[\delta_n]$, and loss due to system failure L. Consider the limit of these systems as the number of vulnerabilities $N \to \infty$, exploit probabilities of individual vulnerabilities $\rho_n \to 0$, $n = 1, .., N$, and average number of successfully exploited vulnerabilities $\rho := \sum_{n=1}^N \rho_n = O(1)$. In this limit:

$$lim_{N \to \infty} (\bar{L}_\xi^{(N)} / L) = 1 - e^{-\rho(\xi)}, \tag{28}$$

where the residual, after employing mitigation strategy $T(\xi)$, average number of exploited vulnerabilities is $\rho(\xi) := \sum_{n:\xi_n = 1} \rho_n$. Formula (27) directly follows from

$ln\prod_{n:\xi_n=1}(1-\rho_n) = \sum_{n:\xi_n=1} ln(1-\rho_n) = -\rho(\xi) + o(1)$ as $N \to \infty$. In limit (28), optimization (24) is equivalent to minimization of the residual average number of successful exploits, given aggregate cybersecurity budget z:

$$\beta(z) = min_{\xi\in\{0,1\}^N}\{\rho(\xi): \sum_{n=1}^{N}(1-\xi_n)c_n \le z\}. \quad (29)$$

Assuming that vulnerabilities $v_1,..,v_N$, are ordered as follows:

$$\rho_1/c_1 \ge \rho_2/c_2 \ge \cdots \ge \rho_N/c_N, \quad (30)$$

solution to optimization problem (24) is

$$S(z) = L[1-e^{-\beta(z)}], \quad (31)$$

where $\beta(z) = \sum_{n=k(z)}^{N}\rho_n$, and $k(z) = max\{m = 0,1,..,N: c_1+..+c_m \le z\}$. Function $\beta(z)$ decreases from $\beta(0) = \rho$ to $\beta(C) = 0$ as security budget z increases from $z = 0$ to the level allowing for elimination of all potential vulnerabilities $z = C := \sum_{n=1}^{N} c_n$. Function $\beta(z)$ is convex for $0 \le z \le C$ due to diminishing return on investment. Consider the following family of functions $\beta(z)$:

$$\beta(z) = (1-z/C)^{\gamma}\rho, \quad (32)$$

where parameter $1 \le \gamma < \infty$ and the residual loss (31) is

$$S(z) = L\left[1-e^{-(1-z/C)^{\gamma}\rho}\right]. \quad (33)$$

Fig. 6 shows family (33) for different $1 \le \gamma < \infty$.

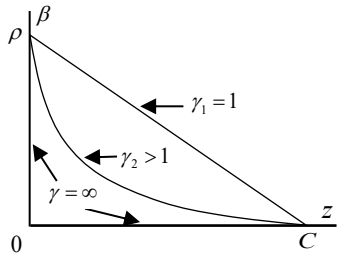
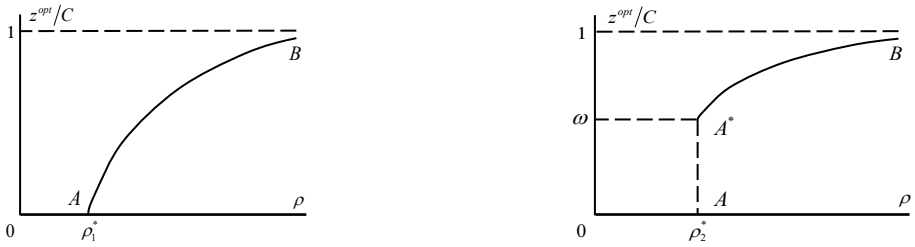


Fig. 6. Function (32) for different $1 \le \gamma < \infty$.

Extreme case $\gamma = 1$ corresponds to a homogeneous system where $\rho_n = \rho/N$, $c_n = C/N$, $n = 1,..,N$, $N \to \infty$. Another extreme case $\gamma \to \infty$ corresponds to the utmost heterogeneous system with $N \to \infty$ potential vulnerabilities, where entire security risk is due to a very small $o(1)$ portion of these vulnerabilities.

The optimal investment z^{opt}, which solves optimization problem (25) for residual risk (33), is shown in Fig. 7a-b.



a. b.

Fig. 7a-b: Optimal investment vs. attack severity ρ.

Parameter space $(L/C, \gamma)$ of this problem can be divided into two regions with optimal investment z^{opt}/C shown in Figures 7a and 7b respectively. Leaving characterization of these regions to the future, here we only claim that these regions are non-empty. System ability to adequately respond to changing level to exogenous threats depends on system ability to efficiently solve microeconomic optimization problem (24).

Our microeconomic model can be viewed as a generalization of model [10] with multiplicative residual risk. We are currently investigating approximate solutions to microeconomic optimization problem (24). We are also generalizing the described in this paper microeconomic model by allowing for a reduction in the probability of successful exploits rather than complete elimination of such a possibility.

References

1. D. Helbing, Globally networked risks and how to respond, *Nature*. 497, 51-59, 02 May 2013.
2. D. Kahneman and A. Tversky, "Prospect Theory: An Analysis of Decision under Risk," *Econometrica*, March, 1979, Vol. 47, No. 2, pp. 263-292.
3. J. Omic, A. Orda, and P. Van Mieghem, "Protecting against network infections: A game theoretic perspective," IEEE INFOCOM 2009.
4. A. R. Hota and S. Sundaram, "Game-theoretic protection against networked SIS epidemics by human decision-makers," IFAC-PapersOnLine, 51 (2019), pp. 145—150.
5. A. Ahmadi-Javid, "Entropic value-at-risk: A new coherent risk measure". Journal of Optimization Theory and Applications. 155 (3), 2012.
6. L.P. Kadanoff, "More is the same; phase transitions and mean field theories," *Journal of Statistical Physics*, Vol. 137, (2009).
7. V. Marbukh, "Towards Landau Theory of Systemic Risk in Large-Scale Networked Systems: Work in Progress," NetSciX'22, Austria, 2022.
8. V. Marbukh, "Systemic Risk of Discontinuous Failures in Large-Scale Networks within Time Horizon: Work in Progress," The 12th International Conference on Complex Networks and their Applications, Menton Riviera, France, November 2023.
9. L. Gordon and M. Loeb, "The Economics of Information Security Investment". ACM Transactions on Information and System Security. 5 (4): 438–457, 2002.
10. Y. Baryshnikov, "IT Security Investment and Gordon-Loeb's 1/e Rule," Workshop on Economics and Information Security, Berlin, June 2012.
11. N. Antunes, C. Fricker, P. Robert and D. Tibi, "Stochastic Networks with Multiple Stable Points," Ann. Probab., Vol. 36, No. 1, 255-278, 2008
12. V. Marbukh. Towards Evaluation & Mitigation of the Entropic Value at Systemic Risk in Networked Systems. 12th International Conference on Complex Networks and their Applications, France, Nov. 28 – 30, 2023.
13. R.E. Kooij, P. Schumm, C. Scoglio, M. Youssef. A new metric for robustness with respect to virus spread, Networking, LNCS 5550, pp. 562–572, 2009.
14. Van Mieghem, P., "Epidemic Phase Transition of the SIS-type in Networks," Europhysics Letters (EPL), Vol. 97, February 2012.
15. V. Marbukh, "Towards Robust Security Risk Metrics for Networked Systems: Work in Progress," 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), Bordeaux, France, 2021.