Reliability Engineering and System Safety 159 (2017) 119–133

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Multiple cyber attacks against a target with observation errors and dependent outcomes: Characterization and optimization

Xiaoxiao Hu[a], Maochao Xu[b], Shouhuai Xu[c], Peng Zhao[d,*]

[a] School of Mathematics and Statistics, Lanzhou University, China
[b] Department of Mathematics, Illinois State University, USA
[c] Department of Computer Science, University of Texas at San Antonio, USA
[d] School of Mathematics and Statistics, Jiangsu Normal University, China

ARTICLE INFO

Keywords:
Copula
Cybersecurity
Defense
Optimal strategy

ABSTRACT

In this paper we investigate a cybersecurity model: An attacker can launch multiple attacks against a target with a *termination strategy* that says that the attacker will stop after observing a number of successful attacks or when the attacker is out of attack resources. However, the attacker's observation of the attack outcomes (i.e., random variables indicating whether the target is compromised or not) has an observation error that is specified by both a false-negative and a false-positive probability. The novelty of the model we study is the accommodation of the *dependence* between the attack outcomes, because the dependence was assumed away in the literature. In this model, we characterize the monotonicity and bounds of the compromise probability (i.e., the probability that the target is compromised). In addition to extensively showing the impact of dependence on quantities such as compromise probability and attack cost, we give methods for finding the optimal strategy that leads to maximum compromise probability or minimum attack cost. This study highlights that the dependence between random variables cannot be assumed away, because the results will be misleading.

1. Introduction

Mathematically modeling and reasoning about cybersecurity is an emerging new research field of high importance, because cyberspace (or the Internet) has become an important pillar underlying economy, human privacy, and even national security. These models aim to describe the interactions between the cyber attacker and the cyber defender at both a microscopic and macroscopic level. Macroscopic cybersecurity models aim to describe, from a whole-system or holistic perspective, the interactions between the various types of cyber attacks and the various types of cyber defenses over a complex network (e.g., [21,35,34,22]). Microscopic cybersecurity models can help cyber defenders make decisions in scenarios that include "one-shot" attack-defense interactions in a centralized [10] or distributed setting [2,18,9], resource allocation against different types of cyber attacks [30,4,33,25], the cost-effectiveness of cyber defenses [7,5,3], and strategic interactions between the cyber attacker and the cyber defender (e.g., [36,26]). We refer to [14] for a comprehensive review of recent developments in the field of microscopic cybersecurity models.

The present study follows a particular microscopic model investigated by Levitin and Hausken [20], which can be applied to both cyberspace and the physical world. This model investigates, from an attacker's point of view, the optimal attack strategy that can cause the maximum damage, while possibly minimizing the cost to the attacker. The novelty of the model is the introduction of the attacker's evaluation errors when determining whether an attack has succeeded or not. The evaluation error indicates that the attacker might have to launch subsequent attacks even if the target is *observed* to have been compromised (or destroyed), simply because the observation can be false. The matter of observation error is relevant in many scenarios. In the context of cybersecurity, imposing false-positive and false-negative observation errors on the attacker represents an emerging defense known as *deception* [27]. Deception aims to mislead the attacker to make ineffective or wrong decisions, but may only succeed with a certain probability. For example, the recently proposed *honey-patch* mechanism aims to cheat an attacker into believing that its attack was successful, while it was not [1]. As another example, the defender can set up fake services to mislead a Distributed Denial-of-Service (DDoS) attacker to believe that the genuine services have been successfully taken offline, assuming that the defender knows how the attacker monitors the outcome of its attacks. This effectively causes a false-positive observation error to the attacker. On the other hand, a false-negative observation error means that the attacker cannot tell that it

[*] Corresponding author.
E-mail address: zhaop@jsnu.edu.cn (P. Zhao).

http://dx.doi.org/10.1016/j.ress.2016.10.025
Received 22 February 2016; Received in revised form 3 October 2016; Accepted 30 October 2016
Available online 12 November 2016
0951-8320/

indeed has successfully compromised a system in question. This can happen, for example, when the attacker uses malware to launch automated attacks, where the attacker knows the attack has succeeded by receiving some “phone home” message from the malware after the malware penetrates into a target system. However, if the defender enforces strong control on the out-bound traffic of the target system, the malware's “phone home” traffic could be blocked and as a result, the attacker does not know the malware has indeed succeeded.

1.1. Our contributions

In this paper, we make two contributions: *conceptual* and *technical*. The conceptual contribution is that we introduce a new perspective into the study of microscopic cybersecurity models, namely the dependence between the relevant random variables. This is demonstrated through a specific model that was studied in [20], where the attack outcomes are assumed to be independent (i.e., the dependence between the corresponding random variables is assumed away). We argue that in many scenarios, we must accommodate the dependence between the relevant random variables, because of the following. To be more specific, let us consider the following two examples where the dependence cannot be ignored:

- Suppose the attacker can launch three Distributed Denial-of-Service (DDoS) attacks from compromised computers under the attacker's control. Suppose the three attacks, when launched independently against a target (e.g., a web server), can compromise the *availability* of the target — an important security property — with probabilities .8, .6, and .4, respectively. Suppose the target survived the first attack launched by the attacker, which causes the defender to block some of the IP addresses from which the DDoS attack was launched. If the attacker launches the second DDoS attack from the same set of IP addresses, the success probability can be reduced to an extent proportional to the number of IP addresses that have been blocked. In this case, the dependence between the attack outcomes is *positive*.
- Suppose the attacker has several attacks (i.e., exploits) that can be launched against a target (e.g., web server). Initially, the attacker may not know exactly what software vulnerabilities the target may possess. After a sequence of unsuccessful attacks, the attacker can ascertain the vulnerabilities of the target and then use the right exploit to compromise the target immediately. In this case, the dependence between the attack outcomes is *negative*.

The technical contribution is that we propose to model the dependence between the relevant random variables in microscopic cybersecurity models via the *copula* technique, which has been widely used in the literature of reliability, finance, statistics, and engineering [15,24]. This is also demonstrated by accommodating the dependence between the attack outcomes in the setting of [20]. Moreover, we tackle two problems that were left open in [20]. The open problems concern the *monotonicity* of the compromise probability (i.e., the probability that the target is compromised) that will be defined later, which was conjectured and supported by numerical evidence but no proof [20]. In this paper, we prove the monotonicity of the compromise probability in the more general model when the dependence is accommodated. Furthermore, we enrich the more general model by investigating two new research aspects, namely the impact of dependence on the compromise probabilities and the expected cost to the attacker. We present bounds on the compromise probability, which are particularly useful when the specific dependence structure between the attack outcomes is not known. We also present methods for identifying the optimal attack strategies, which achieve the maximum compromise probability with a fixed budget, or the minimum cost corresponding to a given compromise probability.

1.2. Related work

In the literature, the topic of defense against the intentional attacks has attracted much attention in recent years. For example, Hausken et al. [13] considered the optimal strategy for allocating the resource to defend a single object against a one-shot intentional and unintentional attacks. Levitin and Hausken [18] and Hausken and Levitin [9] considered the scenario of defending parallel systems subject to two consecutive attacks. They studied the optimal strategy for defending the system with constrained resources. In particular, they considered it as a minmax two period game between the attacker and the defender, and studied the strategy of deploying redundant elements and protecting them against the attacks. Levitin and Hausken [19] considered the optimal sequential attack strategy from the perspective of an attacker. They studied the optimal number of attacks for destroying a system, and also considered the optimal allocation strategy with constrained resources. They discussed multiple scenarios, including: whether one large attack with the entire resource is more powerful than several attacks with equal but smaller resources; whether the attacker should geometrically increasing or decreasing the resource distribution into a fixed number of sequential attacks, or just equally allocate the resource. Later, a more complex scenario was studied in Levitin and Hausken [20], where they considered the attacks with imperfect detection of attack outcomes. That is, the attacker may wrongly identify a destroyed target as undestroyed, and may wrongly identify an undestroyed target as destroyed. The optimal attack strategy was discussed thoroughly based on this model. More recently, Mo et al. [23] studied the optimal strategy of resource allocation between increasing the protection of components and constructing redundant components in parallel systems that are subject to intentional threats. They proposed a dynamic resource distribution strategy with geometric construction pace model. They showed that the dynamic strategy is more effective in reducing destruction probability.

It is worth mentioning that all of the studies mentioned above did not consider the interdependent properties between components of a system. There are only some limited discussion on the defending the dependent systems. For example, Hausken [11] analyzed the dependent system subject to attacks by a strategic attacker via Markov analysis and repeated games. Specifically, it is considered that a successful attack on one target in the first period would impact the other target in the second period on the unit costs and the contest intensity. Wang et al. [32] presented vulnerability analysis for the interdependent infrastructure systems, and discussed three types of attack strategies. Recently, Hausken [12] studied two interdependent targets, where the failure of one target has an impact on the second target. The reliability of system was discussed from the perspectives of players' efforts and expected utilities. One may also refer to the references therein for the related discussion on the dependent system.

However, our work in this paper is different from the work in the literature from two perspectives. First, we consider the dependence among the attack outcomes of a sequential attack. Second, we use the tool of copula to capture the dependence among attack outcomes, which is more flexible. We remark that our approach is different from the multi-stage stochastic programming (MSP) approach in the literature. From the modeling perspective, the MSP approach is mainly used for multi-period optimization models with dynamic stochastic data during the time, which has been used in many areas including production planning, energy, transportation etc. [17,16,29]. It emphasizes on the decision made today given the known information and unknown uncertainty in the future, while the uncertainty is represented via a scenario tree. The objective function is used to represent the risk associated with the sequence of decisions to be made, and then it is converted to a large scale linear or quadratic program (or general convex optimization problem). The main difference is that the MSP approach models the consequences of decisions based on a scenario tree while the copula approach models the dependence among the events. From the technique perspective, the MSP could be viewed as a subclass of finite-horizon Markov Decision processes [29]. It works very well when the optimization of objective function is convex, particularly, for the continuous decision space and the number of decision stages is small [8]. The copula models the multivariate dependence among the events by using the Sklar's theorem, which is very flexible to capture the complicated high-dimensional dependence [15,24].

The rest of paper is organized as follows. In Section 2, we review some concepts and definitions related to copulas. In Section 3, we present our model that accommodates dependence between random variables. In Section 4, we present some analytic results. In Section 5, we present some numerical results. In Section 6, we conclude the paper with some open problems for future research. Some lengthy proofs are deferred to the Appendix.

The following table summarizes the main notations used in the paper:

$\mathrm{P}(\cdot)$, $\mathrm{E}[\cdot]$	the probability and expectation functions
$F_h(\cdot,\ldots,\cdot)$	h-dimensional joint distribution
$C_h(\cdot,\ldots,\cdot)$	h-dimensional copula function
n	a parameter specifying the attacker's termination strategy (i.e., when to stop launching attacks)
D	the event that the target is compromised
D_h	the event that the target is compromised exactly by the hth attack (i.e., the previous $h-1$ attacks all failed but the hth attack succeeds)
N_h	the event that the target is not compromised by the previous $h-1$ attacks
I_h	the event that the number of *observed successful* attacks among the previous $h-1$ attacks is smaller than n, where $h \geq n+1$
S_i	the outcome of the ith attack
T_i	the cost to the attacker (i.e., the amount of resource consumed) for launching the ith attack, where $1 \leq i \leq K$ and K is number of attacks the attacker has
$R = \sum_{i=1}^{K} T_i$	the amount of resources available to the attacker

2. Preliminaries

Copula is widely used for modeling dependence between random variables [15,24]. The idea is to model dependence by relating the multivariate joint distribution to the individual marginal distributions. A function C: $[0, 1]^n \mapsto [0, 1]$ is called a n-copula if it has the following properties:

- $C(u_1,\ldots,u_n)$ is increasing in u_z for $z \in \{1,\ldots,n\}$.
- $C(u_1,\ldots,u_{z-1}, 0, u_{z+1},\ldots,u_n) = 0$ for all $u_j \in [0, 1]$ where $j = 1,\ldots,n$ and $j \neq z$.
- $C(1,\ldots,1, u_z, 1,\ldots,1) = u_z$ for all $u_z \in [0, 1]$ where $z = 1,\ldots,n$.
- C is n-increasing, namely that for all $(u_{1,1},\ldots,u_{1,n})$ and $(u_{2,1},\ldots,u_{2,n})$ in $[0, 1]^n$ with $u_{1,j} \leq u_{2,j}$ for all $j = 1,\ldots,n$, it holds that

$$\sum_{z_1=1}^{2} \cdots \sum_{z_n=1}^{2} (-1)^{\sum_{j=1}^{n} z_j} C(u_{z_1,1},\ldots,u_{z_n,n}) \geq 0.$$

Let $X_1,\ldots,X_n$ be random variables with distribution functions respectively denoted by $F_1,\ldots,F_n$. Consider the joint distribution function $F(x_1,\ldots,x_n) = \mathbb{P}(X_1 \leq x_1,\ldots,X_n \leq x_n)$. The famous *Sklar's theorem* says that there exists a n-copula C such that

$$F(x_1,\ldots,x_n) = C(F_1(x_1),\ldots,F_n(x_n)).$$

There are many copula structures [15,24]. As examples, we will consider the following three families of dependence structures. The first example is the Normal copula

$$C(u_1,\ldots,u_n) = \Phi_{\Sigma}(\Phi^{-1}(u_1),\ldots,\Phi^{-1}(u_n)),$$

where Φ^{-1} is the inverse cumulative distribution of the standard normal distribution, and Φ_{Σ} is the joint cumulative distribution of a multivariate normal distribution with mean vector zero and covariance matrix equal to the correlation matrix Σ. For simplicity, we will assume that the correlation matrix has the form

$$\Sigma = \begin{pmatrix} 1 & \rho & \ldots & \rho \\ \rho & 1 & \rho & \rho \\ \cdots & & & \\ \rho & \rho & \ldots & 1 \end{pmatrix}, \tag{1}$$

where ρ is the correlation between the two relevant random variables. In this case, the Normal copula can be rewritten as

$$C(u_1,\ldots,u_n) = \Phi_{\rho}(\Phi^{-1}(u_1),\ldots,\Phi^{-1}(u_n)). \tag{2}$$

The second example is the t copula, namely

$$C_{\nu,\Sigma}(u_1,\ldots,u_n) = \int_{-\infty}^{t_\nu^{-1}(u_1)} \cdots \int_{-\infty}^{t_\nu^{-1}(u_n)} \frac{\frac{\Gamma(\nu+n)}{2}}{\Gamma(\frac{\nu}{2})\sqrt{(\nu\pi)^n|\Sigma|}} \left(1 + \frac{\mathbf{x}'\Sigma^{-1}\mathbf{x}}{\nu}\right)\mathbf{dx}, \tag{3}$$

where $t_\nu^{-1}(\cdot)$ is the quantile function of the standard univariate t-distribution with degree of freedom v, and Σ is the correlation matrix in the form of Eq. (1). Note that the t copula is similar to the normal copula except that it has one more parameter v, which controls the heaviness of the tail of the distribution.

The third example is the Archimedean copula, namely

$$C(u_1,\ldots,u_n) = \phi^{-1}(\phi(u_1)+\cdots+\phi(u_n)),$$

where ϕ is a generator of C. This family of copulas contains many copula functions such as Clayton and Gumbel [24]:

- Clayton copula: In this case, the generator is $\phi_\theta(u) = u^{-\theta} - 1$, and

$$C(u_1,\ldots,u_n) = \left[\sum_{j=1}^{n} u_j^{-\theta} - n + 1\right]^{-1/\theta}, \quad \theta \& 0. \tag{4}$$

The Clayton copula models a positive dependence, especially a lower-tail dependence.

- Gumbel copula: In this case, the generator is $\phi_\theta(u) = [-\log(u)]^\theta$, and

$$C(u_1,\ldots,u_n) = \exp\left\{-\left[\sum_{j=1}^{n} (-\log(u_j))^\theta\right]^{1/\theta}\right\}, \quad \theta \& 1. \tag{5}$$

The Gumbel copula models a positive dependence, especially the upper-tail dependence.

We use the following concept of *positive lower orthant dependent* to compare copulas.

Definition 1. ([24,15]) Let C_1 and C_2 be two copulas. C_1 is said to be less Positive Lower Orthant Dependent (PLOD) than C_2, or $C_1 \leq_{\mathrm{PLOD}} C_2$, if

$$C_1(u_1,\ldots,u_n) \leq C_2(u_1,\ldots,u_n)$$

for all $0 \leq u_i \leq 1, i = 1,\ldots,n$.Note that both the Gaussian copula and the Clayton copula are increasing in ρ and θ in terms of the PLOD order.

In addition, we use the following stochastic order to compare two random variables.

Table 1
Observation error of attacker: a is the false-negative probability and b is the false-positive probability.

		True attack outcome	
		Success	Failure
Attacker's observation	Failure	a	$1-a$
	Success	$1-b$	b

Definition 2. ([28]) Consider two random variables X and Y with the same support. X is said to be less than Y in the usual stochastic order (denoted by $X \le_{st} Y$) if

$$P(X \le a) \ge P(Y \le a)$$

for all $a \in \mathbb{R}$.

3. The new model accommodating dependent outcomes

The model that assumes independent attack outcomes [20]. In the model, an attacker attempts to compromise (or destroy) a target by launching attacks against it. The attacker has a limited amount of attack resources, say K attacks (e.g., exploits). After launching one attack, the attacker needs to observe whether or not the attack has successfully compromised the target. However, the attacker's observation has two kinds of error: (i) the false-negative probability a, namely the probability that the attacker's observation concludes that the attack is not successful while it is; (ii) the false-positive probability b, namely the probability that the attacker's observation concludes that the attack is successful while it is not. As shown in Table 1, these two kinds of observation errors can be seen as the Type I and Type II errors in statistics. Formally, let S_i denote the outcome of the ith attack, where $i = 1, 2, \ldots, K$, where

$$S_i = \begin{cases} 1, & \text{Success}, \\ 0, & \text{Failure}. \end{cases}$$

An important *assumption* of the model is that the S_i's are independent [20].

Denote by

$$P(S_i = 1) = 1 - P(S_i = 0) = v_i, \quad i = 1, \ldots, K.$$

The success probability v_i is defined via the *contest function* [31] as follows. Suppose the attacker allocates the total amount of resource R into the K attacks. Suppose T_i is the amount of resource allocated for the ith attack, namely $\sum_{i=1}^{K} T_i = R$. Suppose $T_i = qT_{i-1}$ for $i = 2, \ldots, K$ and a given number q. Note that q represents the so-called *geometric resource distribution* [19], where q&1 means that the attacker decreases its attack effort because T_i&T_{i-1}, q=1 means that the resource will be evenly allocated to the attacks, and q&1 means that the attacker increases its attack effort because T_i&T_{i-1}. The success probability of the ith attack is given by the contest function

$$v_i = \frac{T_i^m}{T_i^m + t^m}, \tag{6}$$

where t is the amount of defensive resources allocated by the defender (e.g., the degree of thoroughness in examining the attack traffic), and $m \ge 0$ indicates the intensity of the contest.

The resource mentioned above may be considered as the cost in reality, which has been explained in [19,20]. In the following, we explain the meaning of cost in the context of cyber security, where it is natural to accommodate cost. For example, a cost is imposed on the attacker when the use of deception makes it harder for the attacker to tell the systems that are truly vulnerable from the systems that are not, or because the use of deception that allows the defender to collect information about the attacker and its attack strategies/tactics. One concrete cost is the number of attack tools/mechanisms that have to be used before the attacker reaches a high confidence that the target system is compromised, which happens because of the attacker's false-negative observation error mentioned above. This is important, especially for new or zero-day attacks, because the use or exposure of a new attack tool will allow the defender to become aware of it, meaning that the usefulness of the attack tool can degrade quickly. On the other hand, false-positive observation error can also incur cost to the attacker because the attacker may receive some “phone home” information that was actually tailored to mislead the attacker or hold the attacker accountable (e.g., using decoy documents [27]).

The attacker has a *termination strategy*, which says that the attacker will stop attacking the target when the attacker has exhausted all of its K attacks, or when the attacker has observed n successful attacks (i.e., the attacker observed that n of the attacks it has launched are successful). Regardless of the number of successful attacks the attacker observed, the target can be compromised only once.

Our new model that accommodates dependent attack outcomes while addressing more questions. As mentioned above, an important assumption made in the preceding model is that attack outcomes are independent [20]. As we discussed in the Introduction, this assumption might not hold because the attacks are rarely independent of each other. Given that independent attack outcomes are a special case of dependent attack outcomes, the generalization to accommodating dependence between the attack outcomes is interesting not only from a theoretic perspective but also from a practical perspective. This motivates us to accommodate the dependence between the S_i's as follows. The probability that all of the first h attacks failed to compromise the target is

$$F_h(0, \ldots, 0) = P(S_1 = 0, \ldots, S_h = 0) = P(S_1 \le 0, \ldots, S_h \le 0) = C_h(1 - v_1, \ldots, 1 - v_h), \tag{7}$$

where $C_h(\cdot)$ is a copula for accommodating the dependence between the S_i's. Under the same *termination strategy*, the target is compromised either by some of the first n attacks (while noting that the attacker may observe none or some of the n attacks as successful), or by some of the attacks that are launched afterwards. Therefore, the *compromise probability* can be represented as

$$P(D) = \sum_{h=1}^{n} P(D_h) + \sum_{h=n+1}^{K} P(D_h \cap I_h),$$

where D_h is the event wherein the target is compromised exactly by the hth attack (recalling that the target only needs to be compromised once), and I_h is the event that the number of observed successful attacks among the previous $h-1$ attacks is smaller than n (explaining why the attacker needs to launch further attacks). For $h = 1, \ldots, K$, we have

$$P(D_h) = P(S_1 = 0, \ldots, S_{h-1} = 0) - P(S_1 = 0, \ldots, S_h = 0) = C_{h-1}(1 - v_1, \ldots, 1 - v_{h-1}) - C_h(1 - v_1, \ldots, 1 - v_h). \tag{8}$$

For $h = n + 1, \ldots, K$, we have

$$P(I_h | D_h) = \sum_{s=0}^{n-1} \binom{h-1}{s} b^s (1-b)^{h-1-s}.$$

Putting things together, we have

$$\begin{aligned}
P(D) = &\sum_{h=1}^{n} [C_{h-1}(1-v_1,\ldots,1-v_{h-1}) - C_h(1-v_1,\ldots,1-v_h)]\\
&+ \sum_{h=n+1}^{K}\sum_{s=0}^{n-1}\binom{h-1}{s} b^s(1-b)^{h-1-s}\\
&[C_{h-1}(1-v_1,\ldots,1-v_{h-1}) - C_h(1-v_1,\ldots,1-v_h)]\\
= &\ 1 - C_n(1-v_1,\ldots,1-v_h) + \sum_{h=n+1}^{K}\sum_{s=0}^{n-1}\binom{h-1}{s} b^s(1-b)^{h-1-s}\\
&[C_{h-1}(1-v_1,\ldots,1-v_{h-1}) - C_h(1-v_1,\ldots,1-v_h)].
\end{aligned}$$

In the generalized model with dependence, we address the following important questions: (i) We prove that the *compromise probability* increases with n, the number of observed successful attacks. This monotonicity was shown to hold via numerical evidence but with no proof in [20] for the independent case. (ii) We prove that the *compromise probability* decreases with b, the false-positive probability. This monotonicity was also shown to hold via numerical evidence but with no proof in [20] for the independent case. (iii) We characterize the impact of the dependence on the *compromise probability* and the impact of the dependence on the expectation and variance of the cost to the attacker. We present bounds on the compromise probability, and using numerical examples to show that the bounds are reasonably tight. (iv) We investigate optimal attack strategies, by seeking the minimum attack cost with respect to a given compromise probability or the maximum compromise probability with respect to a given attack cost.

4. Analytic characterization of $P(D)$ and attack cost

4.1. Monotonicity of P(D)

We prove that $P(D)$ increases with the number n of observed successful attacks, decreases with the false-positive probability b, and decreases with the dependence between the attack outcomes (in the PLOD order).

Proposition 1. *$P(D)$ increases with n, namely the number of observed successful attacks.*

Proof. Note that

$$\begin{aligned}
P(D) = &\ 1 - C_n(1-v_1,\ldots,1-v_n) + \sum_{s=0}^{n-1}\binom{n}{s} b^s(1-b)^{n-s}\\
&[C_n(1-v_1,\ldots,1-v_n) - C_{n+1}(1-v_1,\ldots,1-v_{n+1})]\\
&+ \sum_{h=n+2}^{K}\sum_{s=0}^{n-1}\binom{h-1}{s} b^s(1-b)^{h-1-s}\\
&[C_{h-1}(1-v_1,\ldots,1-v_{h-1}) - C_h(1-v_1,\ldots,1-v_h)].
\end{aligned}$$

If the attacker stops after launching the $(n+1)$ th attack, the probability that the target is compromised, denoted by $P(D^*)$, becomes

$$\begin{aligned}
P(D^*) = &\ 1 - C_n(1-v_1,\ldots,1-v_n)\\
&+ [C_n(1-v_1,\ldots,1-v_n) - C_{n+1}(1-v_1,\ldots,1-v_{n+1})]\\
&+ \sum_{h=n+2}^{K}\sum_{s=0}^{n-1}\binom{h-1}{s} b^s(1-b)^{h-1-s}\\
&[C_{h-1}(1-v_1,\ldots,1-v_{h-1}) - C_h(1-v_1,\ldots,1-v_h)].
\end{aligned}$$

Since

$$\sum_{s=0}^{n-1}\binom{n}{s} b^s(1-b)^{n-s} \le 1,$$

it follows that

$$P(D) \le P(D^*).$$

□

Remark 1. Without considering the dependence between the attack outcomes, it was conjectured in [20] that $P(D)$ increases with n. This conjecture was supported by numerical examples, but not a proof. Proposition 1 proves that the conjecture holds even in the more general setting with dependence, of which the independence setting investigated in [20] is a special case.

Proposition 2. *$P(D)$ decreases with b, namely the false-positive probability.*

Proof. Note that

$$P(I_h|D_h) = \sum_{s=0}^{n-1}\binom{h-1}{s} b^s(1-b)^{h-1-s}$$

can be regarded as the binomial distribution with parameters $B(h-1, b)$, i.e,

$$P(Y_{h-1} \le n-1) = \sum_{s=0}^{n-1}\binom{h-1}{s} b^s(1-b)^{h-1-s}, \tag{9}$$

where $Y_{\mathrm{h}-1}$ is a binomial random variable with parameters $h-1$ and b. It is known (e.g., [28]) that

$$B(h-1, b) \le_{st} B(h-1, b^*), \qquad b \le b^*.$$

Therefore,

$$\begin{aligned}
P(D) = &\ 1 - C_n(1-v_1,\ldots,1-v_h) + \sum_{h=n+1}^{K} P(Y\\
&\le n-1)[C_{h-1}(1-v_1,\ldots,1-v_{h-1}) - C_h(1-v_1,\ldots,1-v_h)],
\end{aligned}\tag{10}$$

decreases in $b \in (0, 1)$. □

Remark 2. The intuition behind Proposition 2 is the following: When the false-positive probability b increases, more attacks will be mistakenly observed as successful and consequently the attacker will stop after launching fewer attacks. This monotonicity property was also conjectured with numerical evidence in [20] for the special case that the attack outcomes are independent. Proposition 2 shows that this conjecture holds even in the more general setting where dependence exists between the attack outcomes.

Proposition 3. *Consider two attack outcomes, namely $(S_1, S_2, \ldots, S_K)$ with dependence captured by copula C and $(S_1^*, S_2^*, \ldots, S_K^*)$ with dependence captured by copula C^*. Then,*

$$C \le_{\mathrm{PLOD}} C^* \Longrightarrow P(D) \ge P(D^*).$$

Remark 3. The intuition behind Proposition 3 is the following: when the dependence between the attack outcomes is strong (e.g., two attacks are variants of each other), the defender can learn some useful information from one attack and uses the information to defend more effectively against the variant attack. In other words, the stronger the dependence, the smaller the compromise probability.

To get a better understanding of the proposition, we present the following numerical example.

Example 1. Suppose the attacker has an amount of resource R=2 for launching K=3 attacks, and the defender has an amount of resource t=5. Suppose the dependence structure (S_1, S_2, S_3) is captured by the Clayton copula

$$C_\theta(u_1, u_2, u_3) = \left[\sum_{j=1}^{3} u_j^{-\theta} - 2\right]^{-1/\theta}, \quad \theta\&0.$$

It is known in the literature that

$$\lim_{\theta\to 0} C(u_1, u_2, u_3) = u_1u_2u_3,$$

which corresponds to the independent case, and that

Table 2
The compromise probabilities for different θ's and n's.

θ	.001	.1	.5	.7	1	1.9
n=1	.575	.567	.537	.525	.510	.474
n=2	.643	.631	.592	.576	.555	.508
n=3	.647	.635	.595	.579	.558	.510
θ	3	5	10	20	30	100
n=1	.446	.415	.383	.370	.368	.367
n=2	.471	.430	.388	.370	.368	.367
n=3	.472	.430	.388	.370	.368	.367

$$C_{\theta_1} \leq_{\text{PLOD}} C_{\theta_2}, \quad \theta_1 \leq \theta_2.$$

Consider the following three termination strategies:

- n=1: In this case, the compromise probability is

$$P(D) = 1 - b(1 - v_1) - (1 - b)bC_\theta(1 - v_1, 1 - v_2) - (1 - b)^2 C_\theta(1 - v_1, 1 - v_2, 1 - v_3).$$

- n=2: In this case, the compromise probability is

$$P(D) = 1 - b^2 C_\theta(1 - v_1, 1 - v_2) - (1 - b^2)C_\theta(1 - v_1, 1 - v_2, 1 - v_3).$$

- n=3: In this case, the compromise probability is

$$P(D) = 1 - C_\theta(1 - v_1, 1 - v_2, 1 - v_3).$$

Consider the contest function in Eq. (6) with parameters m=.4, a=.2, b=.2, and q=.4. Then, we have

$$v_1 = .367, \quad v_2 = .287, \quad v_3 = .218.$$

Table 2 summarizes the compromise probabilities for different θ's and n's. We observe that the compromise probability decreases with θ, which confirms Proposition 3. In other words, the more dependence between the attack outcomes, the smaller the compromise probability. Indeed, we observe that the dependence has a significant effect. For example, when n=2, the compromise probability is .643 when $\theta = .001$ (i.e., the dependence between the attack outcome is weak). However, the compromise probability decreases to .367 when $\theta = 100$ (i.e., the dependence between the attack outcomes is strong). We also observe that the compromise probability increases with n, meaning that a strategy requiring the attacker to observe more successful attacks before stopping, leads to a greater compromise probability. However, when the dependence between the attack outcomes is very strong (e.g., θ&10), the effect of n (i.e., the difference between strategies) is small. This interesting phenomenon can be explained by that when θ is large, we have

$$C_3(1 - v_1, 1 - v_2, 1 - v_3) \approx C_2(1 - v_1, 1 - v_2) \approx 1 - v_1,$$

which implies that $P(D) = v_1 = .367$.

4.2. Expected attack cost

In order to characterize the impact of the dependence on the expected attack cost, we observe that the attacker may stop after the jth attack where $j = n, \ldots, K$, and the cost to the attacker is respectively $\sum_{i=1}^{j} T_i$ where T_i is the cost of the ith attack.

Proposition 4. *Let J_n be the number of attacks that have been launched before the attacker stops attacking, the expected cost to the attacker is*

$$\mathrm{E}_n = \sum_{j=n}^{K} P(J_n = j) \sum_{i=1}^{j} T_i,$$

where for $n \leq j \leq K - 1$ we have

$$P(J_n = j) = \binom{j-1}{n-1} b^n (1 - b)^{j-n} C_j(1 - v_1, \ldots, 1 - v_j) + \sum_{h=1}^{j} \sum_{s=0}^{n-1} \binom{h-1}{s} b^s (1 - b)^{h-1-s} \times \binom{j-h}{n-1-s} (1 - a)^{n-s} a^{j-h-n+1+s} \times [C_{h-1}(1 - v_1, \ldots, 1 - v_{h-1}) - C_h(1 - v_1, \ldots, 1 - v_h)] \tag{11}$$

and for j=K we have

$$P(J_n = K) = 1 - \sum_{j=n}^{K-1} P(J_n = j). \tag{12}$$

We present the following example for illustration.

Example 2. Suppose the attacker can launch K=3 attacks. Consider the following two termination strategies.

- n=1: In this case, the possible values for J_1 are 1,2 or 3, and we have

$$P(J_1 = 1) = b(1 - v_1) + (1 - a)v_1, \; P(J_1 = 2) = b(1 - b)C_2(1 - v_1, 1 - v_2) + (1 - a)av_1 + (1 - b)(1 - a)[1 - v_1 - C_2(1 - v_1, 1 - v_2)],$$

and

$$P(J_1 = 3) = (1 - b)^2 C_2(1 - v_1, 1 - v_2) + a^2 v_1 + (1 - b)a[1 - v_1 - C_2(1 - v_1, 1 - v_2)].$$

Hence, the expected attack cost is

$$\mathrm{E} = T_1 + [(1 - b) + (a + b - 1)v_1]T_2 + [a(1 - b) + a(a + b - 1)v_1 - (1 - b)(a + b - 1)C_2(1 - v_1, 1 - v_2)]T_3.$$

- n=2: In this case, the possible values for J_2 are 2 or 3, and we have

$$P(J_2 = 2) = (1 - a)^2 - (1 - a)(1 - a - b)(1 - v_1) - b(1 - a - b)C_2(1 - v_1, 1 - v_2),$$

and

$$P(J_2 = 3) = a(2 - a) + (1 - a)(1 - a - b)(1 - v_1) + b(1 - a - b)C_2(1 - v_1, 1 - v_2).$$

Therefore, the expected attack cost is

$$\mathrm{E} = (T_1 + T_2) + [a(2 - a) + (1 - a)(1 - a - b)(1 - v_1) + b(1 - a - b)C_2(1 - v_1, 1 - v_2)]T_3.$$

Set the parameters as in Example 1, namely R=2, t=5, a=.2, b=.2, q=.4 and m=.4. It can be calculated that

$$T_1 = 1.282, \quad T_2 = .513, \quad T_3 = .205.$$

That is, the first attack uses the most resources, and the next two attacks use much less. Table 3 shows that the expected cost for n=2 is larger than the cost for n=1, which is plausible because the more observed successes leads to a higher cost. We also observe that when the dependence increases (i.e., θ becomes larger), the expected cost also increases. This is the more dependence would lead to smaller compromise probability as shown in Proposition 3, and hence the expected cost would increase. However, the expected cost does not change much when the dependence becomes very large (say, $\theta \geq 10$), because the compromise probability becomes relatively stable when the

Table 3
Expected attack cost for different attack termination strategies.

θ	.001	.1	.5	.7	1	1.9
n=1	1.648	1.648	1.651	1.651	1.653	1.656
n=2	1.942	1.942	1.943	1.943	.1.943	1.944
θ	3	5	10	20	30	100
n=1	1.658	1.66	1.664	1.665	1.665	1.665
n=2	1.945	1.945	1.946	1.947	1.947	1.947

dependence is strong as shown in Table 2.

4.3. Bounding P(D) *when dependence structures are unknown*

In practice, we need to know at least some information about the compromise probability $P(D)$ when the dependence structure is not known. Here we present bounds for $P(D)$ because, for example, the upper bound can be used in the defender's decision-making process.

For this purpose, we first recall a result.

Lemma 1. ([24]) *Let C be any n-copula, then*

$$\max\left\{\sum_{j=1}^{n} u_j - n + 1,\ 0\right\} \le C(u_1, \ldots, u_n) \le \min\{u_1, \ldots, u_n\}.$$

Proposition 5. *The compromise probability P(D) can be bounded as follows.*

$$\max\{v_1, \ldots, v_n\} \le P(D) \le 1 - \sum_{s=n}^{K-1} \binom{K-1}{s} b^s (1-b)^{K-1-s}$$
$$\max\left\{1 - \sum_{j=1}^{n} v_j,\ 0\right\} - \sum_{s=0}^{n-1} \binom{K-1}{s} b^s (1-b)^{K-1-s}$$
$$\max\left\{1 - \sum_{j=1}^{K} v_j,\ 0\right\}.$$

Remark 4. The bounds given in Proposition 5 hold regardless of the dependence structure between the attack outcomes. We observe that if any of $v_1, \ldots, v_n$ is large, then the lower bound would be relatively tight; if $\sum_{j=1}^{K} v_j$ is small, then the upper bound is relatively tight. The result in Proposition 5 is quite useful in practice as it does not require the dependence information. The attacker or defender may simply estimate the minimum or maximum compromise probability for the system based on the compromise probabilities of attacks.In the following, we present some numerical examples for illustrating the bounds and their tightness.

Example 3. Suppose the attacker can launch K=5 attacks, and the dependence between the attack outcomes can be described by the Clayton copula structure with parameter $\theta = 2$ as in the previous examples. Suppose the termination strategy is n=2 (i.e., the attacker stops after observing two successful attacks). The other parameters are set as R=2, m=1, a=.15, and b=.15. Fig. 1 plots the lower and upper bounds of the compromise probability with q=.4 and q=1.3 and varying t's. From Eq. (6) we observe that the success probability of individual attacks, namely v_i, decreases in t. Figs. 1(a) and (b) show that the lower bound is very tight when t is small (i.e., v_i is large), and the upper bound is very tight when t is large (i.e., $\sum_{j=1}^{5} v_j$ is small). This confirms Proposition 5.

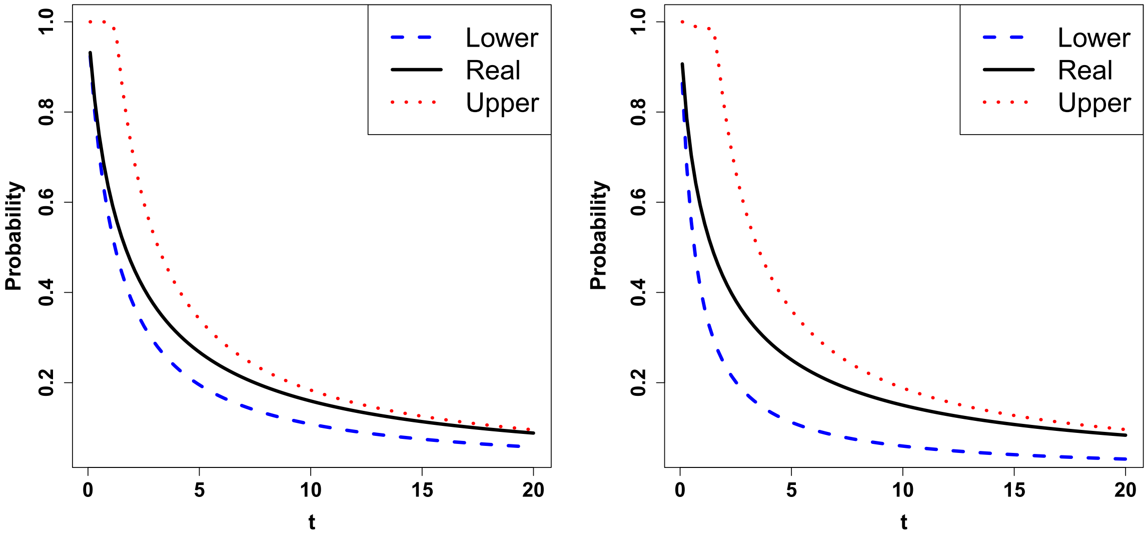
What dependence structure leads to the lower bound of compromise probability? Proposition 5 offers the insight that the defender can impose a certain dependence structure to make $P(D)$ attain or approach its lower bound. It is important for the defender to know which dependence structure can lead or approach to the lower bound, because the defender may be able to impose this dependence structure. In what follows, we discuss a scenario in which $P(D)$ reaches the lower bound. The dependence structure is called *comonotonicity*, which is an extreme form of the positive dependence that is widely used in finance and actuarial science. We mention that comonotonic random variables are always moving in the same direction simultaneously, while referring to Dhaene et al. [6] for a thorough treatment of this property. We start with the following lemma that offers an equivalent characterization of a comonotonic random vector.

Lemma 2. ([6]) *A random vector* $(X_1, \ldots, X_n)$ *is comonotonic if and only if there are increasing real-valued functions* $f_1, \ldots, f_n$ *and and a random variable W such that*

$$(X_1, \ldots, X_n) \overset{st}{=} (f_1(W), \ldots, f_n(W)),$$

where $\overset{st}{=}$ *means that both sides of equality have the same distribution*; *or equivalently*

$$P(X_1 \le x_1, \ldots, X_n \le x_n) = \min\{P(X_1 \le x_1), \ldots, P(X_n \le x_n)\}.$$



(a) Compromise probability when $q = .4$. (b) Compromise probability when $q = 1.3$.

Fig. 1. Lower and upper bounds of compromise probability $P(D)$. (a) Compromise probability when q=.4. (b) Compromise probability when q=1.3.

Proposition 6. *Suppose the dependence between the v_i's has a comonotonic structure, and the largest compromise probability corresponds to one of the first n attacks. Then, the compromise probability equals to the largest compromise probability among the first n attacks.*

Proof. If the largest compromise probability is among the first n attacks, i.e.,

$$m = \arg \max_{i=1,\ldots,K} \{i|0 \le v_i \le 1\},$$

then $1 \le m \le n$. It follows that

$$\begin{aligned} P(D) &= 1 - \min\{1 - v_1, \ldots, 1 - v_n\} + \sum_{h=n+1}^{K} \sum_{s=0}^{n-1} \binom{h-1}{s} b^s (1-b)^{h-1-s} \\ &\quad [\min\{1 - v_1, \ldots, 1 - v_{h-1}\} - \min\{1 - v_1, \ldots, 1 - v_h\}] \\ &= 1 - \min\{1 - v_1, \ldots, 1 - v_n\} = v_m. \end{aligned}$$

This completes the proof. □

In fact, Proposition 6 is confirmed by Example 1, where $v_1 = .367$. As we explained in Example 1, the reason is that the dependence between the attack outcomes is very strong. Proposition 6 presents a formal proof for this phenomena. Proposition 6 may also be used for the attack or defense purpose in practice. For example, if the dependence among the outcomes is known to be strong, Proposition 6 suggests that a large attack with most of the resource may be beneficial to the attacker.

5. Numerical characterizations

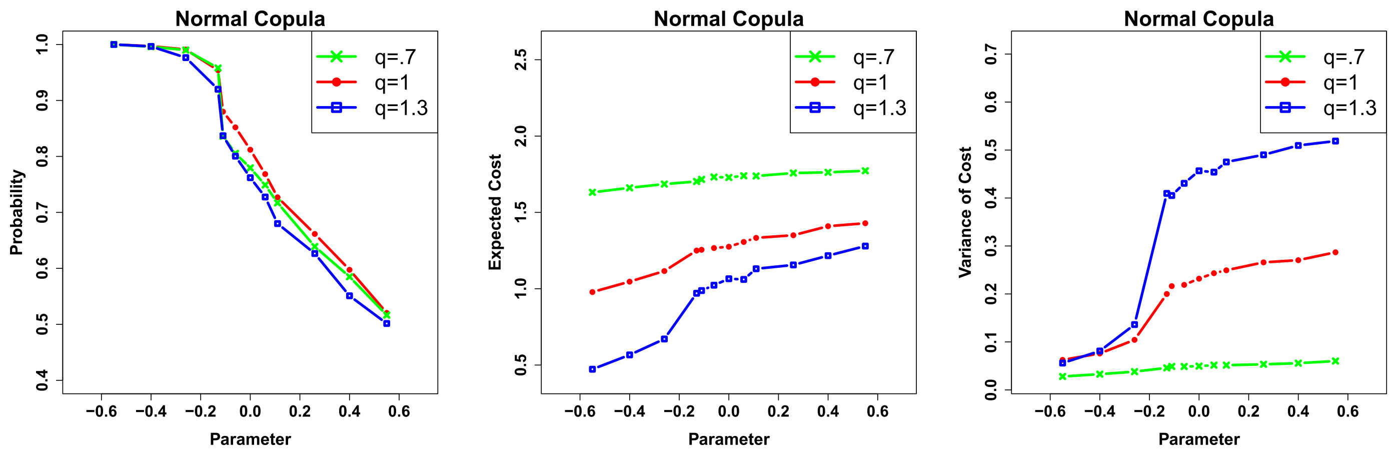
5.1. Impact of the dependence structure on P(D) and attack cost

In the above we have strived to give analytic characterization of the impact of the dependence structure on $P(D)$. Here we give a broader characterization of the dependence structure on $P(D)$ and attack cost, while considering several specific copulas.

Suppose the attacker can launch K=10 attacks, and the termination strategy is n=3. The other parameters are set as $R = 2$, $t = 5$, $m = .5$, $a = b = .2$. In order to evaluate the impact of the dependence structure, we consider $q \in \{.7, 1, 1.3\}$ in the allocation of the amount of resources (i.e., cost) of attacks as well as the Normal, t, Gumbel and Clayton copulas. The simulation algorithm is described in Algorithm 1 (R code is available upon request). The simulations are conducted 2,000 times for calculating the quantities.

Algorithm 1. Simulating the attacks.

```
INPUT: Copula structure $C$ of $(S_1, \ldots, S_K)$; parameters $(n, K, a, b)$; probability vector $(v_1, \ldots, v_K)$
OUTPUT: Attack outcomes
Calculate the non-compromise probability $p_0$ based on copula $C$ for the first $n$ attacks according to Eq.(7)
for $h$=1 to $K$ do
    Calculate the compromise probability $p_h$ according to Eq. (8) with copula $C$
end for
Randomly sample a value $l$ from $(0, 1, \ldots, n)$ according to the probabilities $p_h$'s for $h = 0, 1, \ldots, n$.
if $l == 0$ then
    Generate observed vector $obs_0$: $n$ bernoulli outcomes of 1's with probability $b$
else
    Generate observed vector $obs_1$: $l - 1$ bernoulli outcomes of 1's with probability $b$, and $n - l + 1$ bernoulli outcomes of 1's with probability $1 - a$.
end if
for $s$=$n$ to $K$ do
    if $l == 0$ then
        if $n\&s \le K - 1$ then
            Generate an observed outcome of 1's with probability $b$ for $obs_0$, and create the observed vector $obs$
            Generate a real outcome $r$ of 1 with probability $p_r$.
        end if
    else
        Generate an observed outcome of 1 with probability $1 - a$ for $obs_1$, and create the observed vector $obs$
    end if
    if $\sum obs == n$ then
        return True attack outcomes and observed attack outcomes
    else
        if $r == 1$ and $l == 0$ then
            $l = s + 1$
        end if
    end if
end for
if $\sum obs\&n$ and $s == K$ then
    return True attack outcomes and observed attack outcomes
end if
OUTPUT: Attack outcomes
```



(a) Compromise probability (b) Expected attack cost (c) Variance of attack cost

Fig. 2. The case of the normal copula: Simulation of attack outcomes with different q's and ρ's. (a) Compromise probability (b) Expected attack cost (c) Variance of attack cost.

Table 4
The case of the normal copula: Compromise probability (Prob.), expected attack cost (Exp.), and variance of attack cost (Var) with different q's and ρ's.

	q=.7			q=1			q=1.3		
ρ	Prob.	Exp.	Var	Prob.	Exp.	Var	Prob.	Exp.	Var
−.55	1	1.632	.028	1	.978	.063	1	.473	.056
−.4	.996	1.661	.033	.997	1.047	.076	.997	.567	.081
−.26	.99	1.686	.038	.991	1.116	.104	.977	.671	.136
−.11	.836	1.716	.049	.88	1.255	.216	.837	.988	.407
−.06	.805	1.732	.049	.852	1.267	.219	.8	1.023	.431
0	.78	1.729	.05	.812	1.275	.232	762	1.065	.457
.06	.749	1.74	.052	.769	1.307	.243	.728	1.06	.454
.11	.717	1.738	.052	.727	1.333	.249	.68	1.131	.475
.26	.639	1.758	.053	.662	1.35	.266	.627	1.156	.49
.4	.585	1.762	.056	.598	1.41	.27	.551	1.217	.51
.55	.517	1.773	.06	.521	1.429	.287	.502	1.279	.519

Table 5
The case of t copula: Compromise probability (Prob.), expected attack cost (Exp.), and variance of attack cost (Var) for different q's and ρ's.

	q=.7			q=1			q=1.3		
ρ	Prob.	Exp.	Var	Prob.	Exp.	Var	Prob.	Exp.	Var
−.55	1	1.637	.029	1	.975	.064	1	.471	.053
−.4	.997	1.668	.032	.997	1.058	.082	.996	.548	.075
−.26	.987	1.695	.037	.986	1.119	.106	.985	.68	.129
−.11	.774	1.736	.046	.799	1.292	.23	.751	1.067	.459
−.06	.769	1.728	.05	.782	1.297	.245	.733	1.06	.465
0	.729	1.737	.051	.742	1.312	.25	.715	1.099	.48
.06	.706	1.741	.052	.715	1.33	.244	.692	1.089	.486
.11	.691	1.74	.054	.7	1.36	.257	.643	1.143	.483
.26	.625	1.759	.054	.623	1.397	.262	.584	1.208	.499
.4	.562	1.76	.057	.57	1.413	.282	.518	1.216	.515
.55	.482	1.785	.056	.479	1.465	.287	.455	1.287	.515

5.1.1. The case of normal copula

For the normal copula described in Eq. (2), the dependence is captured by parameter ρ. A negative ρ represents a negative dependence, a positive ρ represents a positive dependence, and $\rho = 0$ represents the independence case. Fig. 2 plots the compromise probability, the expected cost, and the variance of the cost with different ρ's. Table 4 summarizes the values of these quantities.

We make the following observations:

- Compromise probability. Fig. 2(a) shows that all the probabilities decrease with ρ, i.e., the greater the dependence between the attack outcomes, the smaller the compromise probability $P(D)$. This confirms Proposition 3. It is worthy mentioning that the impact of the dependence is significant. For example, when $\rho = -.55$, the compromise probability is 1 and the target is compromised for certain; when $\rho = .55$, the compromise probability drops to 50% in either case of q. Table 4 also shows that the compromise probability is the largest when q=1, namely when attack resources are distributed evenly to the attacks; whereas, the resource allocation method with q=1.3 has the smallest compromise probability.
- Expected attack cost. Fig. 2(b) shows that the expected cost increases with ρ, which is reasonable because the compromise probability decreases with ρ. We also observe that the expected cost is the highest when q=.7 and the lowest when q=1.3.
- Variance of attack cost. Fig. 2(c) shows that the variance of the cost increases with the dependence and the impact of the dependence is significant. For example, the variance when q=1 changes from .063 to .287 when the dependence increases from −.55 to .55. We also observe that the variance is the smallest when q=.7 and the largest when q=1.3.

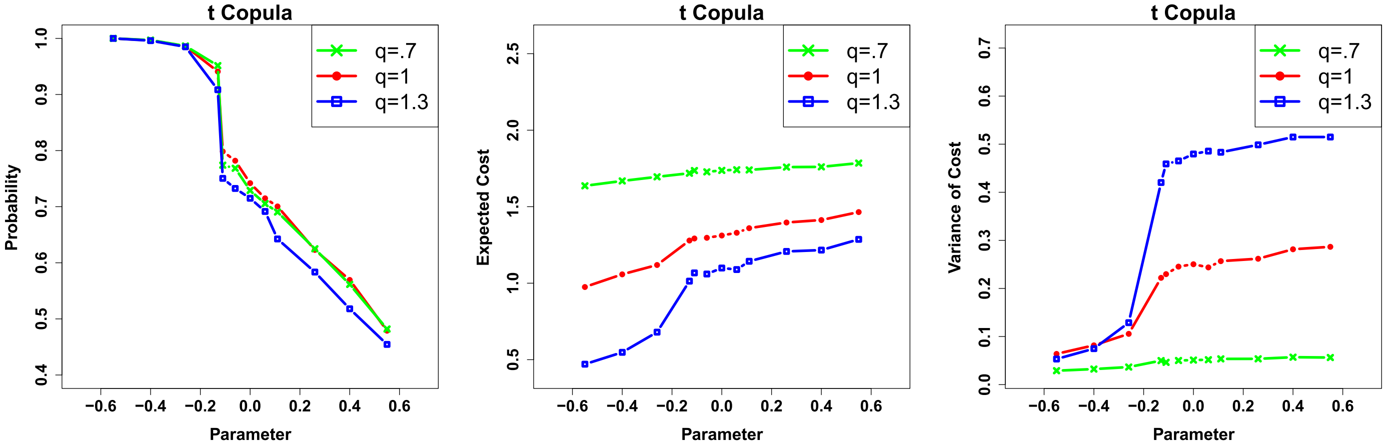
In summary, when the dependence between the attack outcomes follows the normal copula with a strong negative dependence, q=1.3 leads to a relatively high compromise probability with the lowest expected cost. However, if the dependence is positive, q=1 leads to a high compromise probability with a small expected attack cost and a small variance of attack cost.

5.1.2. The case of t *copula*

In this case, we set a small number of nu=5 to model the heavy-tail of distributions. Fig. 3 exhibits a pattern similar to what is exhibited in Fig. 2. By comparing Table 4 and Table 5, we observe that the compromise probability, expected attack cost and variance of attack cost are slightly different, and the dependence has a larger impact on these quantities. In particular, we observe that the compromise probability is smaller when compared with the compromise probability in the case of the normal copula. We can draw a conclusion similar to that of the normal copula case.

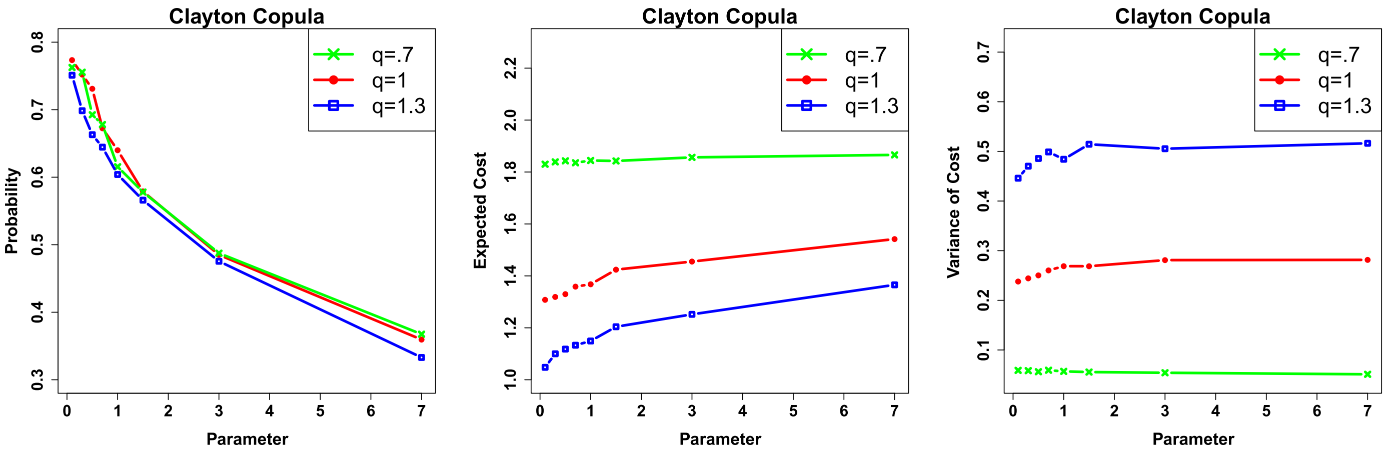
5.1.3. The case of Clayton copula

Fig. 4 plots the simulation results, and Table 6 shows the specific values. We observe that the compromise probability decreases when the dependence increases for all the cases of q's, despite that the probabilities are relatively close to each other. The expected attack cost and the variance of attack cost increase when the dependence increases. For the case q=1.3, the expected cost is the smallest, but



(a) Compromise probability (b) Expected attack cost (c) Variance of attack cost

Fig. 3. The case of t copula: Simulation of attack outcomes with different q's and ρ's. (a) Compromise probability (b) Expected attack cost (c) Variance of attack cost.



(a) Compromise probability (b) Expected cost (c) Variance of cost

Fig. 4. The case of Clayton copula: Simulation of attack outcomes for different q's and ρ's. (a) Compromise probability (b) Expected cost (c) Variance of cost.

Table 6
The case of Clayton copula: Compromise probability (Prob.), expected attack cost (Exp.), and variance of attack cost (Var) for various q's and ρ's.

	q=.7			q=1			q=1.3		
θ	Prob.	Exp.	Var	Prob.	Exp.	Var	Prob.	Exp.	Var
.1	.763	1.83	.059	.774	1.308	.238	.751	1.048	.446
.3	.756	1.839	.058	.752	1.319	.244	.699	1.1	.47
.5	.693	1.843	.056	.731	1.33	.25	.663	1.118	.486
.7	.678	1.836	.059	.673	1.359	.26	.645	1.133	.499
1	.616	1.844	.057	.64	1.368	.269	.604	1.149	.484
1.5	.578	1.843	.056	.579	1.424	.269	.566	1.204	.514
3	.488	1.856	.054	.485	1.455	.281	.476	1.252	.505
7	.368	1.866	.051	.36	1.542	.282	.333	1.366	.516

Table 7
The case of Gumbel copula: Compromise probability (Prob.), expected attack cost (Exp.), and variance of attack cost (Var) for different q's and ρ's.

	q=.7			q=1			q=1.3		
θ	Prob.	Exp.	Var	Prob.	Exp.	Var	Prob.	Exp.	Var
1.1	.721	1.829	.062	.746	1.65	.254	.749	1.642	.254
1.2	.643	1.849	.055	.694	1.636	.263	.68	1.65	.283
1.4	.571	1.85	.054	.58	1.638	.266	.598	1.651	.255
1.6	.51	1.847	.057	.517	1.653	.259	.508	1.658	.253
1.8	.468	1.852	.056	.466	1.651	.255	.48	1.654	.257
2	.423	1.851	.054	.435	1.667	.255	.413	1.683	.237
3	.326	1.864	.051	.291	1.7	.224	.321	1.676	.244
5	.289	1.865	.053	.231	1.692	.23	.26	1.684	.245
7	.287	1.862	.054	.229	1.71	.22	.221	1.687	.245

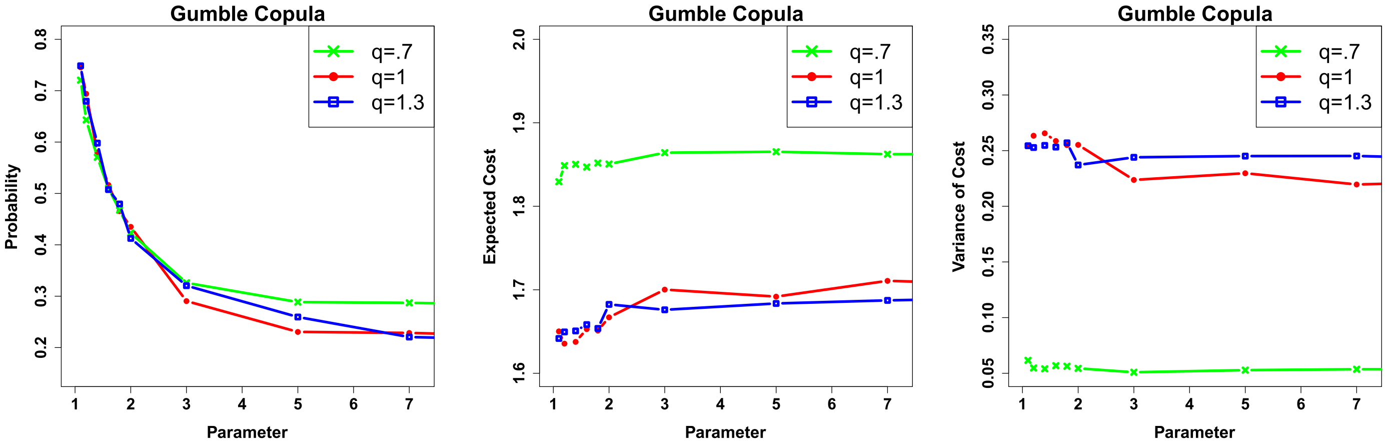
the variance is the largest.

Table 6 suggests that if the dependence can be modeled by the Clayton copula, then evenly distributing attack resources leads to high compromise probability as well as a relatively small expected cost and variance of cost.

5.1.4. The case of gumbel copula

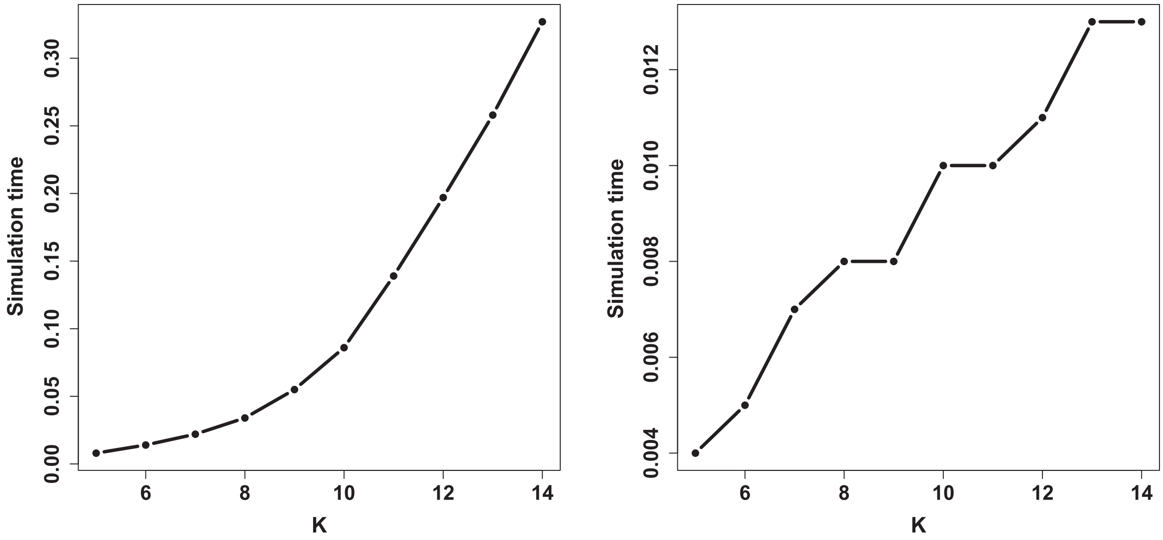
Fig. 5 shows a pattern that is slightly different from the one observed in the preceding cases, see also Table 7. Specifically, the compromise probability decreases with the dependence. When the dependence is strong (i.e., large θ), the compromise probability with q=.7 is the largest. For the expected attack cost, although the overall trend increases in θ, there exist some small oscillations. The expected attack costs with q=1 and q=1.3 are close to each other. For the variance of attack cost, q=.7 leads to the smallest variance, while the variances for the other two cases are about the same.

In summary, the compromise probability decreases with the dependence, as predicted by Proposition 3. From the perspective of the attacker, evenly distributing attack resources is a good strategy if



(a) Compromise probability (b) Expected attack cost (c) Variance of attack cost

Fig. 5. The case of Gumbel copula: Simulation of attack outcomes for different q's and ρ's. (a) Compromise probability (b) Expected attack cost (c) Variance of attack cost.



(a) Normal Copula

(b) Clayton Copula

Fig. 6. Fig. 6(a) and (b) show the time costs of simulation algorithm based on the normal copula and Clayton copula, respectively (time unit: second). (a) Normal Copula (b) Clayton Copula.

the dependence between the attack outcomes is positive. This is because the expected attack cost and the variance of attack cost are relatively low, while the compromise probability is relatively large.

5.1.5. Efficiency of algorithm

In this section, we discuss the solution times of Algorithm 1. The experiment is carried out on a PC with Inter Core i5-4288U CPU and 2.60 GB Ram. To study the efficiency of Algorithm 1, we discuss two cases including the normal and Clayton copulas. The solution times are averaged over 1,000 independent simulation runs.

Fig. 6 shows the mean solution time of the simulation algorithm proposed in the paper, where the time is averaged on 1,000 independent simulation runs. Fig. 6(a) depicts the solution time based on the normal copula, with parameters $m = .5, n = 3, a = .2, b = .2, R = 2, t = 5, q = 1.3, \rho = .55$. The x-axis represents the value of K, and the y-axis represents the solution time. It is seen that the simulation algorithm is very efficient as the time cost is less than .35 s (i.e., negligible). For example, the average solution time for K=14 is only .327 s Fig. 6(b) displays the solution time based on the Clayton copula, with parameters $m = .5, n = 3, a = .2, b = .2, R = 2, t = 5, q = .7, \rho = 10$. Again, we observe that the simulation algorithm is very efficient as well (e.g., .013 s for K=14). Therefore, we conclude that simulation Algorithm 1 is very efficient.

5.2. Optimal attack strategy

Now we discuss the optimal attack strategy under three scenarios of dependence structures: positive, independent, and negative. We use the normal copula for illustration as it is flexible enough to model these scenarios. For the dependence parameter, we set $\rho \in \{.4, 0, -.4\}$ which respectively corresponds to positive, independent and negative dependence. To model the resource allocation of the attacker, we set $q \in \{.7, 1, 1.3\}$, which corresponds to three different resource allocation scenarios. In order to identify the optimal attack strategy, we allow K to vary from 2 to 10, and allow n to take values from $1,\ldots,K$. The other parameters are set as $R = 2, t = 5, m = .5, a = b = .2$.

5.2.1. Minimizing the attack cost with respect to a given compromise probability

Suppose the attacker wants to minimize the expected cost while achieving a compromise probability at least $(1 - \epsilon)$, where the $\epsilon \geq 0$ is a parameter that represents the tolerance of failure. That is

$$\min_{\{K,n,q\}} \mathrm{E}_n \tag{13}$$

subject to

$$\begin{cases} P(D) \geq 1 - \epsilon, & \epsilon \geq 0, \\ \sum_{i=1}^{K} T_i = R, & K \geq 1. \end{cases}$$

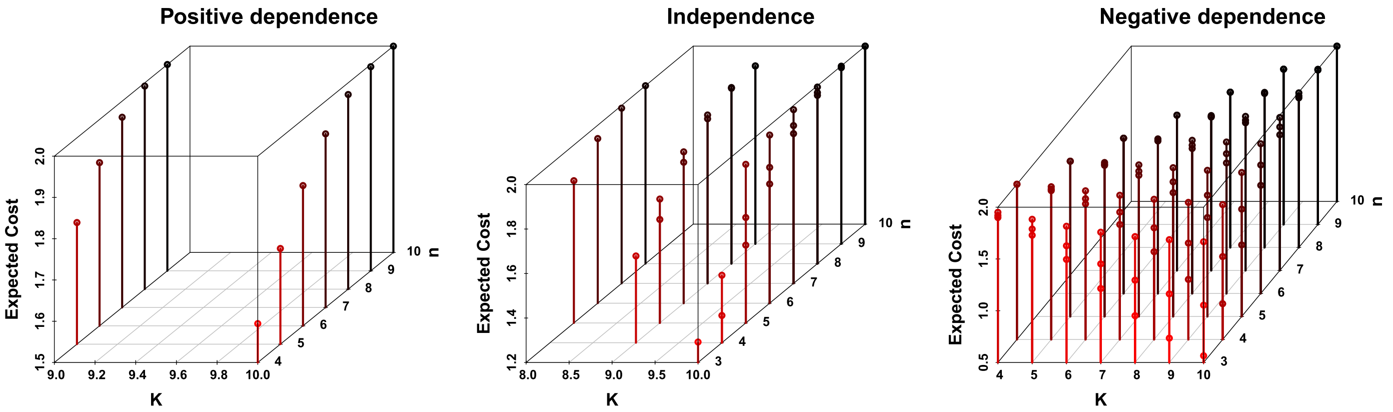
Fig. 7 plots the numerical results. From Table 8 and Fig. 7, we make the following observations.

- Positive dependence: In this case, the summary statistics in Table 8 show that the maximum compromise probability is .6091, which leads to the optimal strategy in Eq. (13) by setting $\epsilon = .4$. Note that for any compromise probabilities greater than .6, the parameter q is always equal to 1 (detailed data is available upon request). This means that the strategy of evenly distributing resources should be used. Fig. 7(a) shows different choices of K, n and the corresponding expected attack costs. We observe that a larger K (i.e., 9 or 10) leads to a smaller expected attack cost. The optimal strategy is $(K, n) = (10, 4)$, while the expected attack cost is 1.594.
- Independence: In this case, Table 8 shows that the maximum compromise probability is .8385. Therefore, for the optimal strategy in Eq. (13), we set $\epsilon = .2$. Fig. 7(b) also shows that a larger K is preferred. The optimal strategy is $(K, n, q) = (10, 3, 1)$, with an expected cost 1.292. That is, attacks should evenly distribute attack resources.
- Negative dependence: In this case, Table 8 shows that the compromise probability is much larger than the preceding cases. For the optimal strategy in Eq. (13), we set $\epsilon = .01$. Fig. 7(c) shows that we have many choices to satisfy the requirement. However, the optimal strategy is $(K, n, q) = (10, 3, 1.3)$, meaning that the attacker should allocate more resources for subsequent attacks.

5.2.2. Maximizing the compromise probability with respect to a given attack cost

Suppose the attacker wants to maximize the compromise probability with a given budget of attack cost. That is,

$$\max_{\{K,n,q\}} P(D)$$



(a) $\rho = .4$ (b) $\rho = 0$ (c) $\rho = -.4$

Fig. 7. Identifying the strategy incurring the minimum cost with a given compromise probability. (a) $\rho = .4$ (b) $\rho = 0$ (c) $\rho = -.4$.

Table 8
Summary statistics of the compromise probability (Prob.) and the expected attack cost (Cost).

	Min	Q_1	Median	Mean	Q_3	Max
$\rho = .4$						
Prob.	.3021	.5242	.5670	.5418	.5854	.6091
Cost	.3913	1.4960	1.8530	1.6800	1.9830	2.0000
$\rho = 0$						
Prob.	.3872	.6585	.7442	.7058	.7897	.8385
Cost	.3386	1.4430	1.8340	1.6510	1.9820	2.0000
$\rho = -.4$						
Prob.	.5142	.9394	1.0000	.9158	1.0000	1.0000
Cost	.1881	1.2970	1.8020	1.5840	1.9810	2.0000

subject to

$$\sum_{i=1}^{K} T_i = R$$

for $K \geq 1$.

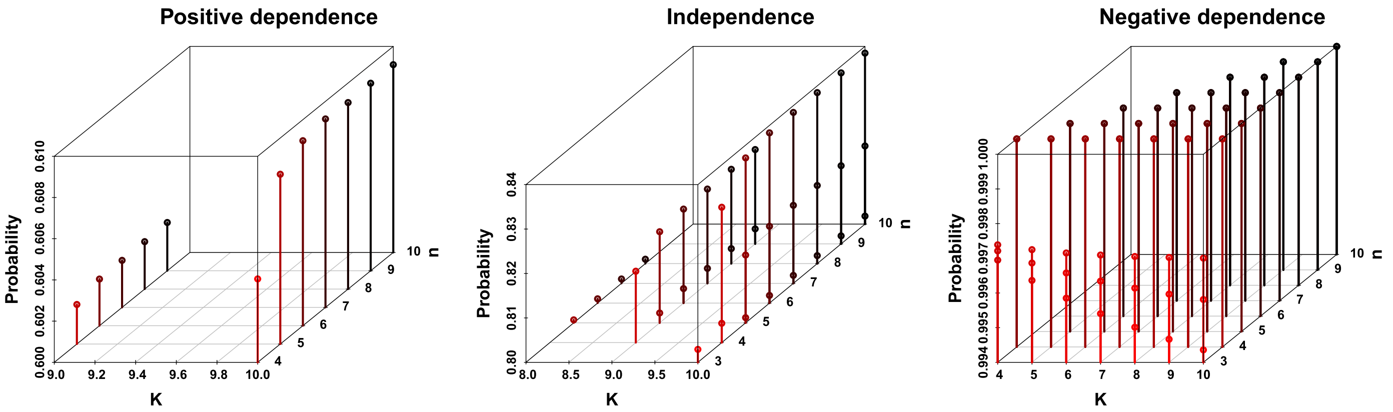
Similar to the previous section, we discuss the optimal strategy for the following three cases.

- Positive dependence. In this case, we plot the compromise probabilities greater than .6 in Fig. 8(a). It is seen that larger K and n are preferred. The largest compromise probability is .609 for the parameter K=10, and n=7. It is worthy pointing out that for K=10 and $n \geq 6$, the compromise probabilities are the same up to three digits. Therefore, the larger K and n's are preferred in this case.
- Independence. In this case, the compromise probabilities greater than .8 are displayed in Fig. 8(b). Again, we observe that larger K and n are preferred. The largest compromise probability is .838 with K=10 and n=10. We also note that when K=10, the compromise probabilities are the same up to three digits for $n \geq 6$. In particular, we observe that q=1 for K=10 and $n \geq 6$. That is, evenly distributing attack resources is preferred.
- Negative dependence. In this case, we plot the compromise probabilities greater than .99 in Fig. 8(c). We see that the largest compromise probability is 1 while the choices of K and n can be different. But considering the expected attack cost, the optimal strategy is $(K, n, q) = (10, 4, 1.3)$ with expected attack cost .846. Therefore, the optimal attack strategy is to use large K and allocate more attack resources to subsequent attacks.

In summary, the optimal strategy for maximizing the compromise probability or minimizing the expected attack cost is to evenly allocate attack resources for positive dependence or independence, but allocate more attack resources to subsequent attacks when the dependence is negative. Moreover, larger K is better from the attacker's perspective, and $n \geq 3$ may be used as the termination rule.

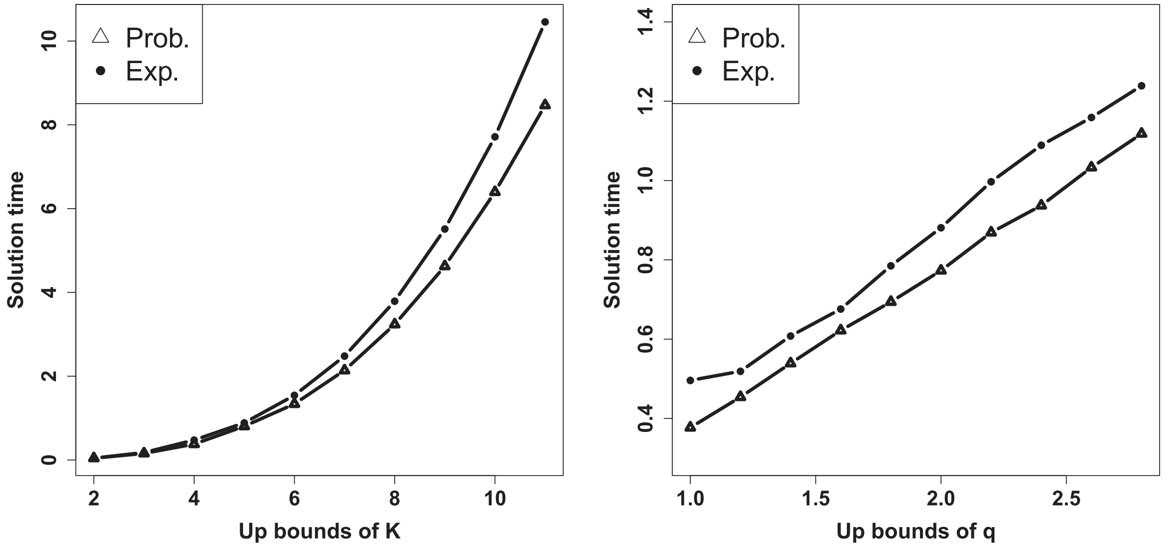
5.2.3. *Efficiency of the optimal frameworks*

In this section, we discuss the efficiency of the optimal frameworks



(a) $\rho = .4$ (b) $\rho = 0$ (c) $\rho = -.4$

Fig. 8. Identifying the strategy incurring the maximum compromise probability with a given budget of attack cost. (a) $\rho = .4$ (b) $\rho = 0$ (c) $\rho = -.4$.



(a) Solution times based on K

(b) Solution times based on q

Fig. 9. Fig. 9(a) and (b) show the time costs of optimal framework based on the normal copula (time unit: second), where Exp. represents the optimal framework in Section 5.2.1, and Prob. represents the optimal framework in Section 5.2.2. (a) Solution times based on K (b) Solution times based on q.

described in Sections 5.2.1 and 5.2.2. Specifically, we discuss the solution time of both frameworks based on the normal copula. Fig. 9 shows the solution time for both frameworks. In Fig. 9(a), we fix the parameters as $\rho = -.7$, $a = .2$, $b = .2$, $m = 1.5$, $R = 3$, $t = 10$, $\epsilon = .12$, and $q \in \{.2, .3, \ldots, 1.0, \ldots, 2.0\}$. The upper bound of K is allowed to vary from 2 to 11. For example, if the upper bound of K is 4, the optimal K value may be any value from 1 to 4. In addition, for any fixed K, the optimal value of n is between 1 and K. For the optimal framework in Section 5.2.1, i.e., minimizing the expected cost while achieving a compromise probability .88, Fig. 9(a) shows that the computational cost is small. For example, corresponding to the upper bound K=11, the solution time is 10.457 s. For the optimal framework in Section 5.2.2, i.e., maximizing the compromise probability with a given budget of attack cost, Fig. 9(a) shows that the computational cost is also small. For example, corresponding to the upper bound K=11, the solution time is 8.468 s. In Fig. 9(b), we use the same parameters $\rho = -.7$, $a = .2$, $b = .2$, $m = 1.5$, $R = 3$, $t = 10$, $\epsilon = .12$, but fix the value of $K \in \{1, 2, 3, 4, 5\}$. We allow the upper bound of parameter q to vary from 1 to 2.8 with an increment .2, and the lower bound of q is set to be .2. After the upper bound is fixed, the optimal value of q is searched from the lower bound with an increment .1 up to the upper bound. For example, if the upper bound of q equals 1.1, the optimal value of q belongs to $\{.2, .3, .4, \ldots, 1.0, 1.1\}$. Fig. 9(b) shows that the computational cost is negligible. For example, for the optimal framework in Section 5.2.1 with upper bound q=2.8, the solution time is 1.239 s. For the optimal framework in Section 5.2.2, the computational cost is 1.118 s

Therefore, we conclude the computational costs of the optimal frameworks in Sections 5.2.1 and 5.2.2 are very small.

6. Conclusion

The domain of cybersecurity is an important area that requires extensive research. Accommodating dependence between random variables in cybersecurity models is a challenging new problem that has yet to be tackled systematically. We have presented a copula-based approach to modeling the dependence between the attack outcomes in a specific cybersecurity model. The theoretical results and simulation-based evidences suggest that the dependence cannot be simply assumed away, because it has a significant impact on the compromise probability and attack cost. We hope this study will inspire future research, including the treatment of the following open problems. The characteristics are presented mainly from the perspective of the attacker, but offer equally useful insights for guiding defensive practices. For example, a negative dependence between the attack outcomes would lead to a greater compromise probability and smaller attack cost; this suggests that the defender should strive to impose positive dependence, which is an exciting problem for future research. Another problem that's worth pursuing is to consider multiple targets, as the present study considers a single target.

Acknowledgement

The authors are grateful to the Associate Editor, and three anonymous referees for their insightful and constructive comments which led to this improved version of the paper. In particular, Sections 5.1.5 and 5.2.3 are from the suggestion of a referee. We thank John Charlton for proofreading the paper. P. Zhao was supported by National Natural Science Foundation of China (11422109), Natural Science Foundation of Jiangsu Province (BK20141145), QingLan Project and A Project Funded by the Priority Academic Program Development of Jiangsu Higher Education Institutions. X. Hu was supported by National Natural Science Foundation of China (11301237, 11571154), and Fundamental Research Funds for the Central Universities (Lzujbky201580). M. Xu and S. Xu was supported by ARO grant (W911NF1310141).

Appendix

Proof of Proposition 3. According to Eq. (10), we have

$$\begin{aligned} P(D) = 1 - &\sum_{s=0}^{n-1}\binom{n}{s}b^s(1-b)^{n-s}C_n(1-v_1,\ldots,1-v_n) - \left[\sum_{s=0}^{n-1}\binom{n}{s}b^s(1-b)^{n-s} - \sum_{s=0}^{n-1}\binom{n+1}{s}b^s(1-b)^{n+1-s}\right]C_{n+1}(1-v_1,\ldots,1-v_{n+1})\vdots \\ &- \left[\sum_{s=0}^{n-1}\binom{K-2}{s}b^s(1-b)^{K-2-s} - \sum_{s=0}^{n-1}\binom{K-1}{s}b^s(1-b)^{K-1-s}\right]C_{K-1}(1-v_1,\ldots,1-v_{K-1}) - \sum_{s=0}^{n-1}\binom{K-1}{s}b^s(1-b)^{K-1-s}C_K(1-v_1,\ldots, \\ &1-v_K) = 1 - P(Y_n \le n-1)C_n(1-v_1,\ldots,1-v_n) - [P(Y_n \le n-1) - P(Y_{n+1} \le n-1)]C_{n+1}(1-v_1,\ldots,1-v_{n+1})\vdots \\ &- [P(Y_{K-2} \le n-1) - P(Y_{K-1} \le n-1)]C_{K-1}(1-v_1,\ldots,1-v_{K-1}) - P(Y_{K-1} \le n-1)C_K(1-v_1,\ldots,1-v_K), \end{aligned}$$

where Y_i is a binomial random variable with parameters i and b. It is shown (e.g., [28]) that

$$B(i, b) \le_{st} B(i+1, b).$$

Therefore, it holds that

$$P(Y_{i-2} \le n-1) \ge P(Y_{i-1} \le n-1)$$

for $i = 3,\ldots,K$. Since

$$C \le_{\text{PLOD}} C^*,$$

it holds that

$$C_i(1-v_1,\ldots,1-v_i) \le C_i^*(1-v_1,\ldots,1-v_i),$$

for $i = 3,\ldots,K$. Therefore, we have

$$P(D) \ge P(D^*).$$

□

Proof of Proposition 4. For $n \le j \le K-1$, we observe that there are $n-1$ observed successes among the previous $j-1$ attacks, while the jth attack is observed as the nth success.

$$P(J_n = j) = P(J_n = j \cap N_j) + \sum_{h=1}^{j} P(\{J_n = j\} \cap D_h) = P(J_n = j|N_j)P(N_j) + \sum_{h=1}^{j} P(J_n = j|D_h)P(D_h).$$

Note that

$$P(J_n = j|N_j) = \binom{j-1}{n-1}b^{n-1}(1-b)^{j-n}b,$$

and

$$P(N_j) = C_j(1-v_1,\ldots,1-v_j).$$

Further, we have

$$P(J_n = j|D_h) = \sum_{h=1}^{j}\sum_{s=0}^{n-1}\binom{h-1}{s}b^s(1-b)^{h-1-s} \times \binom{j-h}{n-1-s}(1-a)^{n-1-s}a^{j-h-n+1+s}(1-a),$$

and recall that

$$P(D_h) = C_{h-1}(1-v_1,\ldots,1-v_{h-1}) - C_h(1-v_1,\ldots,1-v_h).$$

This leads to Eq. (11) and therefore Eq. (12). □

Proof of Proposition 5. For the upper bound, we observe that

$$P(D) = 1 - C_n(1-v_1,\ldots,1-v_n) + \sum_{h=n+1}^{K}\sum_{s=0}^{n-1}\binom{h-1}{s}b^s(1-b)^{h-1-s}[C_{h-1}(1-v_1,\ldots,1-v_{h-1}) - C_h(1-v_1,\ldots,1-v_h)].$$

According to Eq. (9), we have

$$P(Y_{h-1} \le n-1) = \sum_{s=0}^{n-1}\binom{h-1}{s}b^s(1-b)^{h-1-s}.$$

and it holds that (see [28])

$$P(Y_{h-1} \le n-1) \le P(Y_h \le n-1).$$

Therefore,

$$\sum_{s=0}^{n-1}\binom{n}{s}b^s(1-b)^{n-s} \le \sum_{s=0}^{n-1}\binom{h-1}{s}b^s(1-b)^{h-1-s} \le \sum_{s=0}^{n-1}\binom{K-1}{s}b^s(1-b)^{K-1-s}.$$

Then,

$$\begin{aligned}P(D) \le{}& 1 - C_n(1-v_1,\dots,1-v_n) + \sum_{s=0}^{n-1}\binom{K-1}{s} b^s(1-b)^{K-1-s}\sum_{h=n+1}^{K}[C_{h-1}(1-v_1,\dots,1-v_{h-1}) - C_h(1-v_1,\dots,1-v_h)] = 1 - C_n(1-v_1,\dots,\\ & 1-v_n) + \sum_{s=0}^{n-1}\binom{K-1}{s} b^s(1-b)^{K-1-s}[C_n(1-v_1,\dots,1-v_n) - C_K(1-v_1,\dots,1-v_K)] = 1 - \sum_{s=n}^{K-1}\binom{K-1}{s}b^s(1-b)^{K-1-s}C_n(1-v_1,\dots,\\ & 1-v_n) - \sum_{s=0}^{n-1}\binom{K-1}{s}b^s(1-b)^{K-1-s}C_K(1-v_1,\dots,1-v_K) \le 1 - \sum_{s=n}^{K-1}\binom{K-1}{s}b^s(1-b)^{K-1-s}\max\left\{1-\sum_{j=1}^{n}v_j,\, 0\right\}\\ & - \sum_{s=0}^{n-1}\binom{K-1}{s}b^s(1-b)^{K-1-s}\max\left\{1-\sum_{j=1}^{K}v_j,\, 0\right\}\end{aligned}$$

where the second inequality follows from Lemma 1.

For the lower bound, it holds that

$$\begin{aligned}P(D) \ge{}& 1 - C_n(1-v_1,\dots,1-v_n) + \sum_{s=0}^{n-1}\binom{n}{s} b^s(1-b)^{n-s}\sum_{h=n+1}^{K}[C_{h-1}(1-v_1,\dots,1-v_{h-1}) - C_h(1-v_1,\dots,1-v_h)] = 1 - C_n(1-v_1,\dots,1-v_n)\\ & + \sum_{s=0}^{n-1}\binom{n}{s} b^s(1-b)^{n-s}[C_n(1-v_1,\dots,1-v_n) - C_K(1-v_1,\dots,1-v_K)].\end{aligned}$$

Since

$$C_n(1-v_1,\dots,1-v_n) \ge C_K(1-v_1,\dots,1-v_K),$$

we have

$$P(D) \ge 1 - C_n(1-v_1,\dots,1-v_n),$$

i.e.,

$$P(D) \ge \max\{v_1,\dots,v_n\}.$$

□

References

[1] Araujo Frederico, Hamlen Kevin W. Sebastian Biedermann, and Stefan Katzenbeisser. From patches to honey-patches: Lightweight attacker misdirection, deception, and disinformation. In: Proceedings of the 2014 ACM SIGSAC conference on computer and communications security. 2014. p. 942–53.

[2] Bier Vicki, Oliveros Santiago, Samuelson Larry. Choosing what to protect: strategic defensive allocation against an unknown attacker. J Public Econ Theory 2007;9(4):563–87.

[3] Bier Vicki M, Naceur Azaiez M. Game theoretic risk analysis of security threats, vol. 128. Springer Science & Business Media; 2008.

[4] Bier Vicki M, Kosanoglu Fuat. Target-oriented utility theory for modeling the deterrent effects of counterterrorism. Reliab Eng Syst Saf 2015;136:35–46.

[5] Carayon Pascale, Kraemer Sara, Bier VM. Human factors issues in computer and e-business security. In: Abderrahim Labbi, editor. Handbook of integrated risk management for E-Business: measuring, modeling and managing risk. J. Ross Publishing: Fort Lauderdale, FL; 2005.

[6] Dhaene Jan, Denuit Michel, Goovaerts Marc J, Kaas Rob, Vyncke David. The concept of comonotonicity in actuarial science and finance: theory. Insur: Math Econ 2002;31(1):3–33.

[7] Dighe Nikhil S, Zhuang Jun, Bier Vicki M. Secrecy in defensive allocations as a strategy for achieving more cost-effective attacker deterrence. Int J Perform Eng 2009;5(1):31.

[8] Dyer Martin, Stougie Leen. Computational complexity of stochastic programming problems. Math Program 2006;106(3):423–32.

[9] Hausken K, Levitin G. Parallel systems with different types of defence resource expenditure under two sequential attacks. Proc Inst Mech Eng, Part O: J Risk Reliab 2009;223(1):71–85.

[10] Hausken Kjell. Production and conflict models versus rent-seeking models. Public Choice 2005;123(1–2):59–93.

[11] Hausken Kjell. Defense and attack of complex and dependent systems. Reliab Eng Syst Saf 2010;95(1):29–42.

[12] Hausken Kjell. Defense and attack for interdependent systems. Eur J Oper Res 2017;256(2):582–91.

[13] Hausken Kjell, Bier V, Zhuang Jun. Defending against terrorism, natural disaster, and all hazards. In: Bier Vicki M, Azaiez M. Naceur, editors. Game theoretic risk analysis of security threats. Springer: New York; 2009. p. 65–97.

[14] Hausken Kjell, Levitin Gregory. Review of systems defense and attack models. Int J Perform Eng 2012;8(4):355.

[15] Joe Harry. Dependence modeling with Copulas. CRC Press; 2014.

[16] Kall Peter, Mayer János. Stochastic linear programming: models, theory, and computation, vol. 156. New York: Springer Science & Business Media; 2010.

[17] Kallrath Josef, Pardalos Panos M, Rebennack Steffen, Scheidt Max. Optimization in the energy industry. Springer.

[18] Levitin Gregory, Hausken Kjell. Parallel systems under two sequential attacks. Reliab Eng Syst Saf 2009;94(3):763–72.

[19] Levitin Gregory, Hausken Kjell. Resource distribution in multiple attacks against a single target. Risk Anal 2010;30(8):1231–9.

[20] Levitin Gregory, Hausken Kjell. Resource distribution in multiple attacks with imperfect detection of the attack outcome. Risk Anal 2012;32(2):304–18.

[21] Li Yan-Fu, Peng Rui. Service reliability modeling of distributed computing systems with virus epidemics. Appl Math Model 2015;39(18):5681–92.

[22] Mitchell Robert, Chen Ray. Modeling and analysis of attacks and counter defense mechanisms for cyber physical systems. IEEE Trans Reliab 2016;65(1):350–8.

[23] Mo Huadong, Xie Min, Levitin Gregory. Optimal resource distribution between protection and redundancy considering the time and uncertainties of attacks. Eur J Oper Res 2015;243(1):200–10.

[24] Nelsen Roger B. An introduction to copulas, 139. New York: Springer Science & Business Media; 2013.

[25] Peng R, Zhai QQ, Levitin G. Defending a single object against an attacker trying to detect a subset of false targets. Reliab Eng Syst Saf 2016;149:137–47.

[26] Rao Nageswara SV, Poole Stephen W, Ma Chris YT, He Fei, Zhuang Jun, Yau David KY. Defense of cyber infrastructures against cyber-physical attacks using game-theoretic models. Risk Anal 2015.

[27] Salem Malek Ben, Stolfo Salvatore J. Decoy document deployment for effective masquerade attack detection. In: Proceedings of the 8th international conference on detection of intrusions and malware, and vulnerability assessment. 2011. p. 35–54.

[28] Shaked Moshe, Shanthikumar JGeorge. Stochastic orders. New York: Springer Science & Business Media; 2007.

[29] Shapiro Alexander, Dentcheva Darinka, et al. Lectures on stochastic programming: modeling and theory, vol. 16. SIAM, 2014.

[30] Sheeba PS, Ghose Debasish. Optimal resource allocation and redistribution strategy in military conflicts with lanchester square law attrition. Nav Res Logist 2008;55(6):581–91.

[31] Skaperdas Stergios. Contest success functions. Econ Theory 1996;7(2):283–90.

[32] Wang Shuliang, Hong Liu, Chen Xueguang. Vulnerability analysis of interdependent infrastructure systems: a methodological framework. Physica A: Stat Mech Appl 2012;391(11):3323–35.

[33] Wu Baichao, Tang Aiping, Wu Jie. Modeling cascading failures in interdependent infrastructures under terrorist attacks. Reliab Eng Syst Saf 2016;147:1–8.

[34] Xu Maochao, Da Gaofeng, Xu Shouhuai. Cyber epidemic models with dependences. Internet Math 2015;11(1):62–92.

[35] Xu Maochao, Xu Shouhuai. An extended stochastic model for quantitative security analysis of networked systems. Internet Math 2012;8(3):288–320.

[36] Zhuang Jun, Bier Vicki M. Reasons for secrecy and deception in homeland-security resource allocation. Risk Anal 2010;30(12):1737–43.