Response to Multiple Attack Behaviour Models in Cloud Computing

Xu Liu, Xiaoqiang Di(✉), Jinqing Li, Huamin Yang, Ligang Cong, and Jianping Zhao

School of Computer Science and Technology,
Changchun University of Science and Technology, Changchun, China
dixiaoqiang@cust.edu.cn

Abstract. User behaviour models have been widely used to simulate attack behaviour in the security domain. In this paper, we introduce one perfect rational and three bounded rational behaviour models to simulate attack behaviour of attack-defense game in cloud computing, and then discuss defender's response to attacks. We assume cloud provider as the role of defender is intelligent to collect attack-related information so that it can predict attack behaviour model, thus the attack behaviour model is known to defender, we therefore build a single-objective optimization game model to find the optimal virtual machine (VM) monitoring strategy against attacker. Finally, through numerical analysis, we prove that when the attack behavior model is known, the corresponding single-objective optimization game solution is better than the other three solutions.

Keywords: Behaviour model · Attack-defense game
Cloud computing

1 Introduction

Cloud computing provides different services to tenants, such as host service, storage service, application service and so on. Tenants can access and manage cloud services as their own computing resources, this kind of open remote mode is convenient for tenants. Gradually, more and more information is stored in the cloud platform by tenants, which attracts attackers' attention and brings serious security threat to IaaS layer that is the foundation layer of cloud platform [1]. Virtual Machine (VM) is an important IaaS component, it is facing many security incidents such as invading or destroying VM. In addition, if one VM is attacked, users who use it or other VMs that communicate with it, and even its host security will be affected [2]. Therefore, to enhance security of VM has become a problem of both cloud provider and tenants.

To maintain VMs security, cloud provider often collects information on VMs in order to design robust defense against attacks. For example, cloud provider detects intrusion or monitors attack of network system before the invasion of

G. Sun and S. Liu (Eds.): ADHIP 2017, LNICST 219, pp. 489–496, 2018.
https://doi.org/10.1007/978-3-319-73317-3_56

network system harm and then alerts as soon as it detects invasion or attack [3]. It's noteworthy that monitoring will generate cost such as maintenance resource, budget and so on, according to the statistics that a large data center costs range between $10 million to $25 million per year, and maintenance costs up to nearly 80% of the total cost [4]. Hence, monitoring cost can't be ignored, monitoring all VMs may not be the best strategy in consideration of monitoring cost. Since different monitoring strength leads to monitoring resources efficiency for defender, an optimal monitoring strategy balancing cost and monitoring benefit will allow for the saving of the significant resource while minimizing the potential damage inflicted by an unmonitored attack, which is required.

The ultimate objective of monitoring is to respond to attackers. In this paper, we model four types of attack behaviour models: Perfect Rational (PR), (Prospect Theory) PT [5], (Quantal Response) QR [6] and Subjective expected Utility Quantal Response (SUQR) [7], and then analyze how defender will respond to these different attack behaviours in Stackelberg game. In the game, cloud provider playing the role of defender and attacker are two rival game players whose interaction is modelled as repeated games, their payoffs are monitoring or attacking benefit minus operation cost.

From the perspective of defender, if attack behaviour is one of the four models (PR, PT, QR or SUQR), defender will build a corresponding single-objective optimization game model and respond to it according to the game equilibrium strategy.

The main contributions of this paper are as follows:

1. We abstract a trade-off problem between VM monitoring benefit and monitoring cost in cloud computing as a Stackelberg security game problem.
2. The single-objective optimization game equilibrium strategy provides reference to monitor VM for cloud provider.

The structure of this paper is as follows: Sect. 2 introduces the related work researched on single-objective optimization game models; Sect. 3 illustrates the game modelling of the application scenarios and different types of attack behaviour models; Sects. 4 and 5 describe the numerical analysis and summarize this paper.

2 Related Works

There have been many researches about Stackelberg security game based on assumption that attacker is perfect rational, however, sometimes attackers aren't always so perfect rational that they can make the optimal attacking strategy that gives them the maximum utilities. Therefore, more and more researches focus on the bounded rational behaviour model.

1992, Kahneman and Tversky proposed prospect theory (PT) by analyzing behaviour economic, it's innovative that every target's prospect is the composition of value and weight function. 1995, paper [6] first proposed quantal response

(QR) model to control the rationality of the attackers' behaviour by introducing a positive parameter, and then predict the attacking possibility as attacker's response to defender. 2013, paper [7] first put forward subjective expected utility quantal response (SUQR) model, they combined the existing subjective utility functions and QR model proposed before. These three bounded rational user behaviour models are all widely studied. Researches [8,9] summarize and compare the prediction accuracy and performance of PT, QR, SUQR and other user behaviour models used often. These researches mainly focus on the evaluation of prediction accuracy of different attack behaviour models instead of applying them to solve problems.

In order to solve security problems involving different attack behaviours, algorithms [10–13] are designed to calculate the optimal Nash equilibrium strategy based on Stackelberg security game. These researches are concentrated on designing the optimal defense strategy against a single type of attack in a common network environment, however, we apply Stackelberg security game in cloud computing to design VM monitoring strategy based on equilibrium strategy. Meanwhile, many literatures are studied with a restraint that the amount of security resources available is limited [14], different from them, we relax the assumption that security resources are limited since resources in cloud computing are allocated dynamically and relatively cheaper than physical resources.

3 Game Modelling

3.1 Why Use Game Theory?

Game theory is a tool used to analyze how two rival players make decisions from their individual perspectives, especially used more in the security domain recently. We consider a scenario including a cloud provider (the role of defender) and a malicious user (the role of attacker), they belong to two opposing roles without any cooperation. The rivalry between attacker and defender makes their interaction suitable to model as a 1-vs-1 non-cooperative Stackelberg attack-defense game. Attacker selects some or all targets to launch attacks with an attack probability distribution over the target set. Defender tries to monitor VMs that are lean to be attacked in the form of monitoring service time, network traffic peak, data packet content, etc. with a monitor probability distribution over targets set.

In this paper, we focus on finding defender's optimal monitoring probability distribution from a mathematical view instead of monitoring measure. Both attacker and defender will try their best to collect more information about the other side's action. For instance, defender will design monitoring strategy based on attack-related information collected previously, attacker will plan attacking strategy according to the defense-related information collected previously. There will be repeated strategy-making interactions between defender and attacker until a group of monitoring and attacking probability distributions that can satisfy their payoff maximum is reached.

3.2 Payoff

Payoff is the main element in game theory that reflects player's return in every round of action. The payoff of attacker and defender on a target i is shown in Table 1. Two row variables represent attacker's two actions (Attack and Not Attack) and two column variables represent defender's two actions (Monitor and Not Monitor). The payoffs brought to both attacker and defender in each pair of attack and defense action set are separated by commas, the former represents attacker's payoff while the latter represents defender's payoff.

Table 1. Payoff of two players on target i

	Monitor (q_i)	Not monitor ($1-q_i$)
Attack p_i	$-\alpha P_i^a + (1-\alpha)R_i^a - C_i^a$, $\alpha R_i^d - (1-\alpha)P_i^d - C_i^m$	$R_i^a - C_i^a$, P_i^d
Not attack ($1-p_i$)	0, $-C_i^m$	0, 0

The expected payoffs of both attacker and defender are inseparable with respective actions and results thereof (e.g. whether the attacking action is detected by the defender), we use α to define the probability that the attacks are successfully detected. For example, for a target i, if defender monitors that the attacker launches an attack on i, defender will be rewarded by R_i^d; otherwise, defender will be punished by P_i^d. Similarly, attacker will be punished by P_i^a in former case; attacker will be rewarded by R_i^a in later case. The respective expected payoffs of defender and attacker are obtained by accumulating the payoffs from each group of different action set, as shown in Eqs. (1) and (2).

$$U_D(p,q) = \sum_{i\in \mathrm{T}} p_i q_i [\alpha R_i^d + (1-\alpha)\, P_i^d - C_i^m] + p_i(1-q_i)P_i^d$$
$$-(1-p_i)q_i C_i^m = \sum_{i\in \mathrm{T}} q_i[\alpha p_i (R_i^d - P_i^d) - C_i^m] + p_i P_i^d \tag{1}$$

$$U_A(p,q) = \sum_{i\in \mathrm{T}} p_i q_i [\alpha P_i^a + (1-\alpha)R_i^a - C_i^a] + p_i(1-q_i)*$$
$$(R_i^a - C_i^a) = \sum_{i\in \mathrm{T}} p_i[\alpha q_i (P_i^a - R_i^a) + (R_i^a - C_i^a)] \tag{2}$$

Nash Equilibrium: In a game $G = \{s_1, .., s_n; u_1, ..., u_n\}$ with n players, if strategy profile $\{s_1^*, ..., s_n^*\}$ satisfies each player i that s_i^* is the optimal strategy or the strategy that is not worse than other $(n-1)$ strategies, then this strategy profile is called a Nash Equilibrium [15].

In order to find the equilibrium strategy of the Stackelberg game in this paper, we combine the optimization methods of Matlab to develop new algorithm. When attack behavior model is perfect rational, payoff function is linear constrained, we use linprog algorithm; otherwise, we use genetic algorithm (GA).

3.3 Attack Behaviour Model

Attackers are often human beings or agents governed by human beings whose behaviours are not certain. According to recent researches, attack behaviours can be classified into two main categories based on attacker's rationality. If an attacker can design the strategy that provides it the maximum payoff, it will be defined as perfect rational; otherwise, it will be defined as bounded rational. For example, intelligent attackers usually collect information about adversarial information (monitoring strategy or defense measure), but sometimes they can't collect all information, or they aren't always capable of learning defender's exact strategy, which leads that they are unable to design the best strategy that provides them the maximum payoff. In this subsection, we introduce four types of attacker behaviour models that differentiate with attacker's rationality, one perfect rational and three bounded rational: PT, QR, SUQR.

Table 2. Four attack behaviour models

Behaviour model	Attack probability
Perfect Rational (PR)	$p_i = \arg\max U_A, \quad p_i \in [0,1]$
Prospect Theory (PT)	$prospect(i) = \pi(q_i)V * (P_i^a - C_i^a) + \pi(1-q_i)V * (R_i^a - C_i^a)$ $p_i = \frac{prospect(i) - \min(prospect(i))}{\sum_{i=1}^{n}(prospect(i) - \min(prospect(i)))}, \quad \sum p_i = 1$
Quantal Response (QR)	$p_i = \frac{e^{\lambda U_A(q_i)}}{\sum_{j=1}^{n} e^{\lambda U_A(q_j)}}, \quad \sum p_i = 1$
Subjective expected Utility Quantal Response (SUQR)	$p_i = \frac{e^{w_1 R_i^a + w_2 P_i^a + w_3 q_i}}{\sum_{j=1}^{n} e^{w_1 R_i^a + w_2 P_i^a + w_3 q_i}}, \quad \sum p_i = 1$

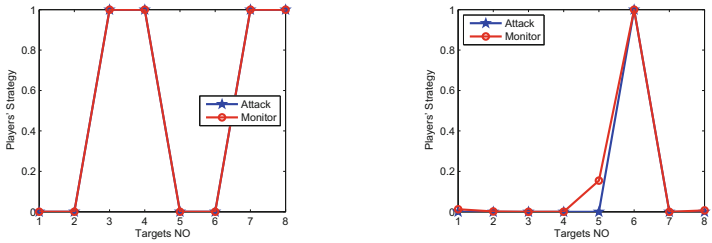
4 Numerical Analysis

In this section, we will perform numerical analysis of single-objective optimization game solutions on 8 targets in Matlab, we set $R_a, R_d \in [0,10]$, $P_a, P_d \in [-10,0]$ used in [12], attack cost C_a and monitor cost C_m both belong to $(0,1)$. These numbers can be exchanged with money or other units of measurement in a real cloud system. We take two experiments with attack-monitor probability distribution, as well as attacker's and defender's utility.

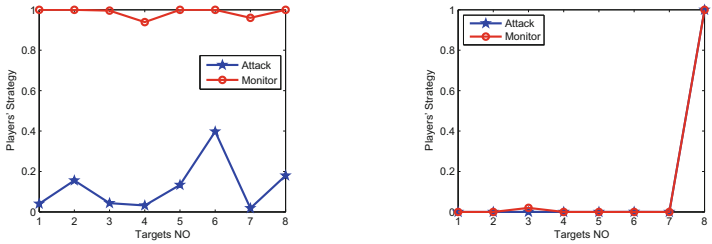
4.1 Players' Strategy

When attack behaviour model is a single type and known to the defender, the defender will build a corresponding single-objective optimization game. In this subsection, we show attack and monitoring strategy in equilibrium status in Fig. 1.

It can be observed that in Fig. 1(a), when attacker is PR, defender's monitoring strategy is consistent with attacker's strategy; once defender predicts that



(a) Perfect Rational (b) Prospect Theory



(c) Quantal Response (d) SUQR

Fig. 1. Players' strategy with four attack behaviour models

Table 3. Player's strategy with QR model

Target NO	1	2	3	4	5	6	7	8
Attack	0.0405	0.155	0.043	0.032	0.134	0.398	0.018	0.180
Descend	6th	**3th**	**5th**	**7th**	**4th**	**1st**	**8th**	2nd
Monitor	0.99966	0.99992	0.99565	0.93916	0.99986	0.99995	0.96029	0.99985
Descend	4th	**2nd**	**6th**	**8th**	**3th**	**1st**	**7th**	5th

target NO. 3,4,7,8 will be attacked with a bigger probability, it will monitor these targets; the same trend can be seen in Fig. 1(b), (c) and (d). In Fig. 1(c), the trend isn't clear, hence, we show the specific values in Table 3, it's easy to find that except two items (target 1 and 8) bigger attack probability is, bigger monitoring probability will be; on target 6, attack probability is the biggest among 8 targets and the corresponding monitoring probability is the biggest that is close to 1. In addition, since defender's monitoring probability distribution is between 0.99 and 1 that difference is so small, thus it's acceptable that the order of monitoring probability isn't the same as the order of attack probability. Meanwhile, compared with the other three subfigures, we can observe that, in QR model, attack probabilities on 8 targets are all bigger than 0 and monitoring probability are all close to 1, which reflects that defender is very careful to avoid missing attack.

According to the monitoring probability distribution, cloud provider can design monitoring methods with different strength or defense measures.

4.2 Players' Utility

As shown in Table 4, four row variables represent four attack probabilities that fit in with four attack behaviour models, four column variables represent four monitoring probabilities calculated from four corresponding single-objective optimization games models. Every cell represents defender's utility gained from the corresponding row attacking and column monitoring probability. Take one cell as an example, while attack probability fits in with PR, single-objective optimization solution (Res_PR) gives defender utility valued as 23.4956 that is the biggest value of the four values of its row.

Table 4. Defender's utility with four attack behaviour models

	Res_PR	Res_PT	Res_QR	Res_SUQR
PR	**23.4956**	−11.4183	21.186	1.2972
PT	−6.5044	**6.1938**	3.6514	−5.4841
QR	−4.7896	−1.7931	**3.0629**	−4.5116
SUQR	6.0956	−5.1484	4.5550	**7.1159**

It's seen from the Table 4 that for every attack behaviour model, the corresponding game solution can bring more monitoring utility for defender than the other three game solutions. Since single-objective optimization game focuses on a single clear objective that maximizes defender's utility. Therefore, we conclude that the corresponding game solution may be the best reference for cloud provider to design optimal VM monitoring strategy.

5 Conclusion

In this paper, we solve the utility-based trade-off problem that includes resource consumption and monitoring benefit by formulating Stackelberg security game. Cloud provider and attacker are modelled as two rival roles of defender and attacker in the game. Specially, we model four types of attack behaviours including PR, PT, QR, SUQR and then study how defender responds to these four attack behaviours. Through numerical analysis we prove that defender's monitoring probability on a target is consistent with the probability that it will be attacked, and appropriate game solution can bring defender more utility. Finally, defender responds to attacks by referring to the Nash Equilibrium strategy of the single-objective optimization security game, bigger equilibrium monitoring probability on a target is, more resource or attention will be paid on it.

Acknowledgment. This research is partially supported by research grants from Science and Technology Project of Jinlin province (20150204081GX). The authors are thankful to reviewers that help to improve the quality of this paper.

References

1. Kaufman, L.M.: Can public-cloud security meet its unique challenges? IEEE Secur. Privacy **8**(4), 55–57 (2010)
2. Kamhoua, C.A., et al.: Game theoretic modeling of security and interdependency in a public cloud. In: IEEE 7th International Conference on Cloud Computing, pp. 514–521 (2014)
3. Chen, L., Leneutre, J.: A game theoretical framework on intrusion detection in heterogeneous networks. IEEE Trans. Inf. Forensics Secur. **4**(2), 165–178 (2009)
4. Saha, S., et al.: A novel revenue optimization model to address the operation and maintenance cost of a data center. J. Cloud Comput. **5**(1), 1–23 (2016)
5. Tversky, A., Kahneman, D.: Advances in prospect theory: cumulative representation of uncertainty. J. Risk Uncertainty **5**(4), 297–323 (1992)
6. McKelvey, R.D., Palfrey, T.R.: Quantal response equilibria for normal form games. Games Econ. Behav. **10**(1), 6–38 (1995)
7. Nguyen, T.H., Yang, R., Azaria, A., Kraus, S., Tambe, M.: Analyzing the effectiveness of adversary modeling in security games. In: AAAI (2013)
8. Abbasi, Y.D., et al.: Human adversaries in opportunistic crime security games: evaluating competing bounded rationality models. In: Proceedings of the Third Annual Conference on Advances in Cognitive Systems ACS, p. 2 (2015)
9. Shieh, E.A., et al.: PROTECT: an application of computational game theory for the security of the ports of the United States. In: AAAI (2012)
10. Kar, D., Fang, F., Delle Fave, F., Sintov, N., Tambe, M.: A game of thrones: when human behaviour models compete in repeated Stackelberg security games. In: Proceedings of International Conference on Autonomous Agents and Multiagent Systems, pp. 1381–1390. AAMAS (2015)
11. Yang, R., Ordonez, F., Tambe, M.: Computing optimal strategy against quantal response in security games. In: Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems, vol. 2, pp. 847–854. AAMAS (2012)
12. Yang, R., Kiekintveld, C., Ordóñez, F., Tambe, M., John, R.: Improving resource allocation strategies against human adversaries in security games: an extended study. Artif. Intell. **195**, 440–469 (2013)
13. Yang, R., Kiekintveld, C., Ordonez, F., Tambe, M., John, R.: Improving resource allocation strategy against human adversaries in security games. In: IJCAI Proceedings-International Joint Conference on Artificial Intelligence, p. 458 (2011)
14. Qian, Y., Haskell, W.B., Tambe, M.: Robust strategy against unknown risk-averse attackers in security games. In: Proceedings of International Conference on Autonomous Agents and Multiagent Systems, pp. 1341–1349. AAMAS, Istanbul, Turkey (2015)
15. Gibbons, R.: A Primer in Game Theory. Harvester Wheatsheaf, Loughborough (1992)