On the Detection of Passive Malicious Providers in Cloud Federations

Ahmad Hammoud, Hadi Otrok, Azzam Mourad, Omar Abdel Wahab, and Jamal Bentahar

***Abstract*— Cloud federation has emerged as a new business architecture which aims to help cloud providers cope with the increased waves of demands on their resources and services. Although plenty of solutions have been proposed trying to ensure the optimal formation of cloud federations, these approaches ignore the problem of encountering malicious providers that join federations to destroy them from inside and exclude some strong competitors from the market. To tackle this challenge, we propose, in this letter, a maximin game theoretical model which assists the broker, responsible for creating and managing federations, with maximizing the detection of such malicious providers. The challenge here is to deal with providers that try to minimize the detection maximization through distributing their misbehavior over several federations and changing their identities from time to time. Experiments conducted using real data from the CloudHarmony dataset reveal that our solution maximizes the detection of malicious providers and improves the profit and quality of service of the federations compared with the sky federation model.**

***Index Terms*— Cloud federation, game theory, security.**

I. Introduction

CLOUD Federations (CFs) are based on the idea of joining together the computing resources of two or more cloud providers in order to increase their capacity of handling an increased number of customers' requests [7]. Such an architecture is beneficial for both providers and customers. From the customers' perspective, the overall Quality of Service (QoS) delivered to their requests will be significantly improved as a result of the increased interoperability among providers. From the providers' perspective, CFs give providers the opportunity to increase their revenue by allowing them to sell or rent their additional (under-utilized) computing resources. Moreover, through CFs, providers will have the chance of expanding their geographical subsistence in new territories without having to build new points-of-presence.

Several approaches have been proposed in the literature in an effort to find the optimal way of forming federations. Mashayekhy *et al.* [5] introduced a dynamic cloud federation formation mechanism which keeps merging and splitting the set of possible federations until reaching the federation which yields the highest monetary profit. Halabi and Bellaiche [3] proposed a cloud federation formation model in which they take into account the security level of each cloud provider, using a hedonic coalitional game. Their proposed algorithm enables the providers to join federations with minimal security risk. In [2], a set of mathematical equations which assist providers in making optimal decisions in terms of possible federations to join so as to maximize the individual providers' profit is advanced.

However, the main limitation of all these works is that they ignore the problem of encountering passive malicious providers in the formed federations. Different from active malicious providers which seek to directly harm other providers/federations, passive malicious providers aim at illegally increasing their own benefits and hence gaining advantage over the other providers. Specifically, a passive malicious provider might misbehave by promising to provide a certain amount of VMs to the federation(s) and then reneging on these promises to dedicate those VMs to the provider's own requests. These passive malicious providers aim at increasing their own profits through outsourcing requests to other providers in the federation but refraining from helping back to save their own resources. Note that the problem of passive malicious providers has been addressed in [8]. However, the main difference between the work done in [8] and our work is that the former aims at excluding the passive malicious providers at the formation's level, but they do not advance any detection mechanism to capture their presence after federations have been formed.

To deal with these shortcomings, we propose in this letter a maxmin game theoretical model [6] that helps the cloud broker[1] maximize the detection of passive malicious providers. The broker's responsibilities include defining the corresponding regulations and standards among cloud providers, distributing the profits yielded by the federations, and ensuring the security of the federations (including the detection of passive malicious providers) under a limited amount of resources. The strategy of the passive malicious providers is to distribute their misbehavior over a set of federations with the aim of maximizing their success chances. In this way, the malicious behavior will not be concentrated in only one (or a few) federation(s) to avoid being easily detected by the broker. On the other hand, given a limited amount of resources that can be dedicated to passive malicious providers detection, the broker's strategy is to distribute the monitoring load over the set of federations to minimize the passive malicious providers' attack

Manuscript received October 2, 2018; accepted October 20, 2018. Date of publication October 30, 2018; date of current version January 8, 2019. The associate editor coordinating the review of this paper and approving it for publication was M. Khabbaz. *(Corresponding author: Azzam Mourad.)*

A. Hammoud and A. Mourad are with the Department of Computer Science and Mathematics, Lebanese American University, Beirut 1102 2801, Lebanon (e-mail: azzam.mourad@lau.edu.lb).

H. Otrok is with the Center for Cyber-Physical Systems, Department of ECE, Khalifa University, Abu Dhabi 127788, United Arab Emirates, and also with the Concordia Institute for Information Systems Engineering, Concordia University, Montreal, QC H3G 1M8, Canada.

O. Abdel Wahab and J. Bentahar are with the Concordia Institute for Information Systems Engineering, Concordia University, Montreal, QC H3G 1M8, Canada.

Digital Object Identifier 10.1109/LCOMM.2018.2878714

[1]According to NIST, a broker is responsible of providing services to the cloud consumers, such as managing hosting environment and cloud infrastructure, in addition to provisioning the physical processing storage, and many other fundamental computing resources [4].

success chances maximization, while not exceeding the limited amount of resources. The main contributions of this letter can be summarized by the following points:

- Designing a maxmin game theoretical model between the cloud broker and the passive malicious providers. By solving the game, the broker learns the optimal distribution of the monitoring load over the set of federations that maximizes the probability of detecting passive malicious misbehavior. To the best of our knowledge, this work is the first that addresses the existence of passive malicious providers in the cloud federations architecture and proposes an intelligent resource-aware detection mechanism to limit their effect on the profitability of the federation.
- Helping cloud providers maximizing their overall monetary profit by joining federations, while allowing customers enjoying improved QoS for their requests.

The rest of the letter is organized as follows. Section II represents the formulation of the problem. Section III explains the approach. Section IV shows experiment results. Finally section V provides the conclusion.

II. Problem Formulation

We consider a set of federations $F = \{f_1, f_2, \ldots, f_n\}$ that are formed to serve a pool of requests from cloud users. Each federation consists of a set of providers $P = \{p_1, p_2, \ldots, p_k\}$ offering a set of virtual machines $V = \{v_1, v_2, \ldots, v_l\}$, where each cloud provider is considered to be part of a certain federation if it dedicates one or more virtual machines to that federation. A cloud provider, according to NIST, is responsible of providing services to the cloud consumers in terms of infrastructure, computing, and storage [4]. Providers may be either well-behaving or malicious. A cloud provider is considered to be well-behaving if it actually dedicates the proclaimed virtual machines to the federations it is member of. While, on the other hand, a cloud provider is said to be malicious if it lies about the number of VMs it will provide with the aim of saving resources and/or dedicating more resources toward fulfilling requests coming from its own users. Note that in this letter we consider only the passive malicious misbehavior in which providers try to gain illegal advantage over other providers and increase their own market share of requests. Thus, active malicious attacks (e.g., Denial of Service) are out of the scope of this work.

To complicate the process of detection, a malicious provider can split its misbehavior over several federations in the sense that it can join federations with multiple identities and misbehave (i.e., provide VMs less than promised) with a small probability and with different identities in more than one federation instead of concentrating its misbehavior on one federation, where it can be easily captured. To deal with such a type of malicious providers, the broker of the cloud federations is responsible, in our architecture, of monitoring the behavior of the cloud providers in the federations. The broker however has a limited amount of resources to be spent on the detection process. The reason is that the broker gets paid by the providers forming the federations to perform this task, where obviously these providers put a certain limit on the amount of money they will spend on this process in such a way that does not greatly affect their overall profit. Thus, the broker must exploit the available resources in an efficient manner by splitting the detection load over the existing federations so as to maximize the detection of malicious providers and respect at the same time the available resources constraints.

Formally, let $\beta_{t,F} = \{\beta_t(f_1), \beta_t(f_2), \ldots, \beta_t(f_n)\}$ denote the misbehavior probability distribution over the set F of joined federations at time t. It depicts the probability that a federation will misbehave. In order to cope with that, and with the limited amount of available resources that the broker possesses to be used for detection, he will have to set a mixed scheme corresponding of the optimum detection load probability distribution vector $\alpha_{t,F} = \{\alpha_t(f_1), \alpha_t(f_2), \ldots, \alpha_t(f_n)\}$ over the set of federations F at time t, such that $\sum_{f_i \in F} \alpha_t(f_i) = 1$.

III. Detecting Passive Malicious Providers

The profit of the federations is mainly dependent on users' satisfaction, which is practically reflected through the monetary payment and the reputation score given by users to the federations. This means that the broker should always make sure that malicious providers are being detected in order to maintain high satisfaction levels from users. Mathematically, the payoff of the federation set F at the discrete time window $[t_1, t_2]$ is determined as follows:

$$U_{t_2+1}(F) = \sum_{f_i \in F} \delta(f_i) \times R(f_i) \times \gamma(f_i)_{[t_1,t_2]} \tag{1}$$

where $\delta(f_i)$ is the profit obtained through renting out the virtual machines of federation f_i which can be calculated by subtracting the total cost of the VMs from the total revenue, $R(f_i)$ is the reputation score of the federation f_i which is computed proportionally to the availability of the federation, and $\gamma(f_i)_{[t_1,t_2]}$ is the average detection rate at the time window $[t_1, t_2]$ that can be computed as the following:

$$\gamma(f_i)_{[t_1,t_2]} = \sum_{\epsilon=t_1}^{t_2} \frac{\beta_\epsilon(f_i) \times \alpha_\epsilon(f_i)}{t_2 - t_1} \tag{2}$$

The calculations in the rest of the letter will be all done at the current time $t_2 + 1$, so we can simplify $U_{t_2+1}(F)$, $\alpha_{t_2+1,F}$, and $\beta_{t_2+1,F}$ by referring to them as $U(F)$, α_F, and β_F respectively. Since the malicious providers' objective is to cause damage to the federations to increase their own market shares, the payoff of the malicious providers can be modeled as being the negation of the federations' utility, i.e.,

$$U(M) = -U(F) \tag{3}$$

where $U(M)$ and $U(F)$ represent the utilities of the malicious providers and the federations respectively. This leads us to zero-sum games in which one player's payoff is the negation of the other player's payoff [6], since the objective of the broker is to maximize profit, while the objective of the malicious provider is to harm and reduce the federations' payoff, this implies that the utility of the former is the negation of the latter's. In order for the malicious provider to succeed with its passive attack and minimize the federation's payoff, it must

choose its probability distribution β_F over the federations' set wisely in such a way to complicate the broker's detection process and hence minimize the federations' utility, i.e.,

$$arg \min_{\beta_F} U(F) \tag{4}$$

On the other hand, the broker must choose the detection probability distribution α_F over the federations' set in order to maximize the malicious providers' minimization and hence maximize the federations utility, i.e.,

$$arg \max_{\alpha_F} \min_{\beta_F} U(F) \tag{5}$$

This forms a maximin game theoretical model in which the malicious providers are trying to minimize the federations' payoff to increase their own market share, and the broker, acting on behalf of the federations, is trying to choose the optimal detection strategy that maximizes the providers' minimization. The solution of the game can be obtained using Linear Programming, where the objective function of the broker can be rewritten as follows:

$$\begin{aligned} &\text{maximize } \min_{\beta_F} \sum_{f_i \in F} \alpha(f_i) \times U(F) \\ &\text{subject to } \sum_{f_i \in F} \alpha(f_i) = 1, \\ &\qquad \alpha(f_i) \geq 0, \quad \forall f_i \in F \end{aligned} \tag{6}$$

To linearize the above equation, we define a variable y such that $y \leq \min_{\beta_F} \sum_{f_i \in F} \alpha\,(f_i) \times U(F)$ and try to make y as large as possible. The problem becomes:

$$\begin{aligned} &\text{maximize } y \\ &\text{subject to } y \leq \sum_{f_i \in F} \alpha(f_i) \times U(F), \\ &\qquad \alpha(f_1) + \alpha(f_2) + \ldots + \alpha(f_n) = 1, \\ &\qquad \alpha(f_i) \geq 0, \quad \forall f_i \in F \end{aligned} \tag{7}$$

To make it easier, we assume that $y{>}0$ and $x(f_i) = \frac{\alpha(f_i)}{y}$, which transforms the constraint $\alpha(f_1) + \cdots + \alpha(f_n) = 1$ into $x(f_1) + \ldots + x(f_n) = \frac{1}{y}$. Now, y can be eliminated by minimizing $x(f_1) + \ldots + x(f_n)$ instead of maximizing y, since maximizing y is equivalent to minimizing $\frac{1}{y}$. The problem becomes:

$$\begin{aligned} &\text{minimize } x(f_1) + x(f_2) + \ldots + x(f_n) \\ &\text{subject to } 1 \leq \sum_{f_i \in F} x(f_i) \times U(F), \\ &\qquad x(f_i) \geq 0, \quad \forall f_i \in F \end{aligned} \tag{8}$$

This problem can be solved using the simplex method in order to derive the optimal monitoring load probability distributions $\alpha(f_i)$ over the set of federations [1]. Our solution will still work well even if the percentage of the malicious providers was 100% because we are able to distribute the detection load to maximize the detection rate regardless of that percentage in one single federation.

IV. Experimental Evaluation

In this section, we evaluate the performance of our solution through comparing it experimentally with the sky federation model [5] since the authors use related configurations and metrics, and to examine the performance of their approach under a harsh environment wherein multiple malicious providers are involved.

A. Implementation Setup

The simulations have been conducted in a 64-bit windows 10 environment having an i7-4720 HQ CPU, 2.6 GHZ, and 16 GB of memory. We used MATLAB as a programming language to implement the two studied models. To compare our solution with the sky federation model, we used a similar setup in terms of VMs prices and configurations (i.e., small, medium, large, and extra-large). We simulated ten cloud providers and varied the percentage of malicious providers from 10% to 50% out of the ten considered providers. Malicious providers would drop some requests coming from the federations with a probability varying from 50% to 99%. The simulations have been run for 100 iterations to maximize the accuracy of the obtained results. To study the performance of our solution w.r.t the sky federation model, five performance metrics have been evaluated, namely those of false negative, attack detection rate, overall profit, latency, and availability. False negative represents the proportion of times in which the model wasn't able to detect a passive malicious action, and which can be calculated as follows:

$$\theta_{[t_1,t_2]} = \sum_{\epsilon=t_1}^{t_2} \sum_{f_i \in F} \frac{\beta_\epsilon(f_i) \times (1 - \alpha_\epsilon(f_i))}{t_2 - t_1} \quad for\ each\ \beta_\epsilon(f_i) > \alpha_\epsilon(f_i) \tag{9}$$

On the other hand, attack detection rate represents the proportion of times in which the model was successful in detecting the passive malicious actions. The overall profit represents the monetary gain yielded by a certain provider as a result of joining a federation. Latency describes the delay between the submission of a user request to a certain VM and the receipt of the response. Finally, availability represents the percentage of times in which a VM was available to serve users requests.

To populate the QoS metrics of the VMs, we used data obtained from CloudHarmony,[2] which records the promised as well as the actual QoS metrics of different cloud services (measured for a period of 30 days) pertaining to different well-known providers such as Amazon and Agile Cloud. This allows us to have an idea about the behavior of the providers in terms of committing to their QoS promises.

B. Results and Discussion

We notice from Fig. 1 that when the percentage of malicious providers increases, the performance of the detection and the QoS decreases. The reason is it becomes harder for the broker to distribute the same budget of detection load over a larger set of attacking virtual machines.

In the first series of experiments, we evaluate the performance of our solution in terms of passive malicious misbehavior detection (Fig. 1a). Note that for this set of experiments

[2]http://cloudharmony.com/

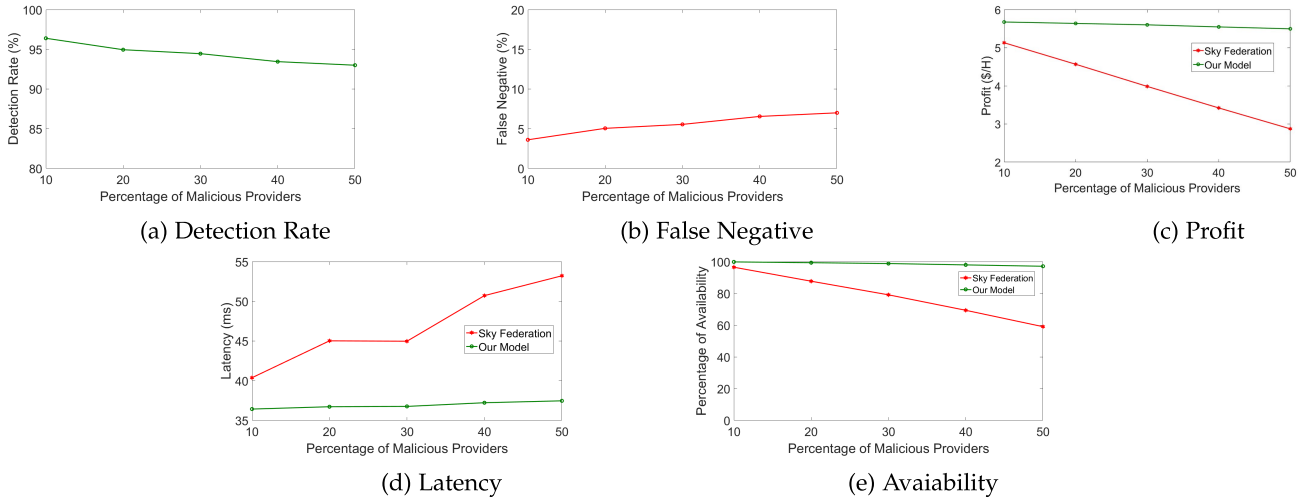

Fig. 1. Experimental results.

the sky federation model wasn't included in the comparisons since this latter model is entirely business-oriented and does not account for the malicious misbehavior when forming federations. By looking at Fig. 1a, we can notice that our solution achieves high detection rates while being scalable to an increased percentage of malicious providers. For example, when the percentage of malicious providers was 10% of the total number of considered providers, the attack detection percentage was 97%. When the percentage of malicious providers jumped to 50%, the attack detection percentage remained high (i.e., 93%). Similarly, Fig. 1b reveals that our solution entails low levels of false negative and its performance is scalable to the increase in the percentage of malicious providers.

In Fig. 1c, we measure the profit per hour yielded by providers compared to the sky federation model. To do so, we injected some malicious providers in the sky federation model and implemented their merge-and-split federation formation algorithms. We can notice from Fig. 1c that our model can increase the profit of the providers in the presence of passive malicious providers compared to the sky federation model. The reason is that we advance a detection strategy to capture the passive malicious misbehavior whose presence leads to decreased performance and hence decreased profit for the federations. In contrary, the sky federation model is purely business-oriented and ignores the existence of malicious providers, which might lead to the generation of federations consisting of a large number of malicious members.

Thereafter, we measure the QoS delivered by the formed federations while serving users' requests. Latency can be defined as the delay from the submission of the user's request to the federation to the submission of the response back to the user. Fig. 1d shows that our solution stabilizes the latency compared to the sky federation model since the malicious providers will be motivated, due to the detection mechanism, to not misbehave under the threat of being penalized. In contrary, the sky federation model gives those malicious providers the freedom to carry out their selfish misbehavior without being detected. Finally, we measure in Fig. 1e, the percentage of availability for the formed federations, where it shows that our solution can improve the availability of the federations compared to the sky model, while being resilient to an increased percentage of malicious providers.

V. Conclusion

In this letter, we addressed the problem of detecting passive malicious providers who join cloud federations to harm the performance, profit, and reputation of those federations. As a solution, we proposed a maximin game theoretical model which allows the cloud broker to maximize the detection of such malicious providers. Experiments conducted using the CloudHarmony dataset show that our solution achieves a high detection rate up to 92% and improves the profit, availability, and latency of the federations up to 25% compared to the sky federation model.

References

[1] T. S. Ferguson, "Game theory," Dept. Math., UCLA, Los Angeles, CA, USA, Tech. Rep., 2008.
[2] I. Goiri, J. Guitart, and J. Torres, "Characterizing cloud federation for enhancing providers' profit," in *Proc. IEEE 3rd Int. Conf. Cloud Comput. (CLOUD)*, Jul. 2010, pp. 123–130.
[3] T. Halabi and M. Bellaiche, "Towards security-based formation of cloud federations: A game theoretical approach," *IEEE Trans. Cloud Comput.*, to be published.
[4] M. Hogan, F. Liu, A. Sokol, and J. Tong, "NIST cloud computing standards roadmap," NIST, Gaithersburg, MD, USA, NIST SP 500-291, 2011, pp. 6–11, vol. 35.
[5] L. Mashayekhy, M. M. Nejad, and D. Grosu, "Cloud federations in the sky: Formation game and mechanism," *IEEE Trans. Cloud Comput.*, vol. 3, no. 1, pp. 14–27, Jan./Mar. 2014.
[6] P. C. Ordeshook, *Game Theory and Political Theory: An Introduction*. Cambridge, U.K.: Cambridge Univ. Press, 1986.
[7] B. Rochwerger *et al.*, "The reservoir model and architecture for open federated cloud computing," *IBM J. Res. Develop.*, vol. 53, no. 4, pp. 4:1–4:4, 2009.
[8] O. A. Wahab, J. Bentahar, H. Otrok, and A. Mourad, "Towards trustworthy multi-cloud services communities: A trust-based hedonic coalitional game," *IEEE Trans. Services Comput.*, vol. 11, no. 1, pp. 184–201, Jan. 2018.