Resource Allocation for Security Services in Mobile Cloud Computing

Hongbin Liang[1,2], Dijiang Huang[3], Lin X. Cai[2], Xuemin (Sherman) Shen[2], Daiyuan Peng[1]
[1]School of Information Science and Technology, Southwest Jiaotong University, {dypeng}@swjtu.edu.cn
[2]Department of Electrical and Computer Engineering, University of Waterloo, {hbliang, lcai, xshen}@bbcr.uwaterloo.ca
[3]School of Computing Informatics and Decision Systems Engineering, Arizona State University, {dijiang}@asu.edu

***Abstract*—Mobile cloud is a machine-to-machine service model, where a mobile device can use the cloud for searching, data mining, and multimedia processing. To protect the processed data, security services, i.e., encryption, decryption, authentications, etc., are performed in the cloud. In general, we can classify cloud security services in two categories: Critical Security (CS) service and Normal Security (NS) service. CS service provides strong security protection such as using longer key size, strict security access policies, isolations for protecting data, and so on. The CS service usually occupies more cloud computing resources, however it generates more rewards to the cloud provider since the CS service users need to pay more for using the CS service. With the increase of the number of CS and NS service users, it is important to allocate the cloud resource to maximize the system rewards with the considerations of the cloud resource consumption and incomes generated from cloud users. To address this issue, we propose a Security Service Admission Model (SSAM) based on Semi-Markov Decision Process to model the system reward for the cloud provider. We, first, define system states by a tuple represented by the numbers of cloud users and their associated security service categories, and current event type (i.e., arrival or departure). We then derive the system steady-state probability and service request blocking probability by using the proposed SSAM. Numerical results show that the obtained theoretic probabilities are consistent with our simulation results.**

I. Introduction

Mobile cloud computing relies on a machine-to-machine computing model, in which mobile devices outsource their computing tasks to the cloud [1]. In this work, our research focuses on the resource allocation for security services of mobile cloud (such as authentication, digital signature, audition, etc.) to mobile devices. Fig. 1 shows the basic structure of mobile cloud service provisioning. In specific, when a mobile device requests a security service to the cloud, the system admission control model consults the system resource management model about the availability of system resource, i.e., Virtual Images (VIs) in our following discussion. Each VI manages a portion of cloud system resources (CPU, storage, etc.). If there are available VIs and the request is accepted, then a VI or several VIs will be allocated to that security service by the system resource management model.

In this paper, we consider that there are two types of security services, as shown in Fig. 1: (i) Critical Security (CS) service, and (ii) Normal Security (NS) service. In [2], the authors had pointed out that in order to provide cloud security service, it is necessary to provide resource isolation among different cloud users. This is especially critical for security services since sharing resources (e.g., memory) enable attackers to explore the system vulnerability [3]. To provide enhanced security services, we need to separate the resources (i.e., VIs) allocated for different security processes owned by different users. In other words, each of CS and NS service subscribers will be allocated a unique VI or unique VIs when he/she requests the cloud resources.

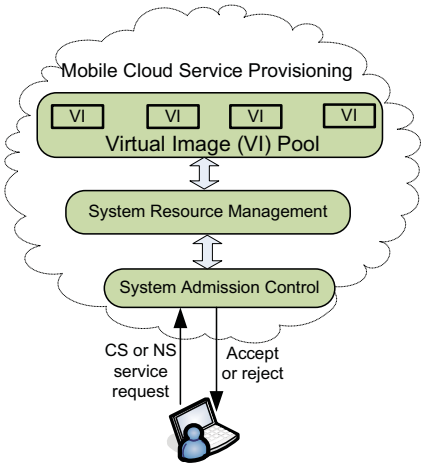

Fig. 1. Reference Model of Mobile Cloud Computing.

To construct an efficient resource allocation model for mobile cloud security services, we present an admission control mechanism based on the total cloud system reward, which takes into account both the cloud income and the cost of the resource occupation. Thus, the system reward is computed in the system resource management model based on the following factors: (i) the arriving and departing rates of CS and NS services, (ii) the numbers of running CS and NS services in the system, (iii) the available total system resource (measured by the numbers of VIs), (iv) the reward for CS or NS service. In general, the CS service involves more complex security implementations such as stronger authentication and encryption algorithms, longer key size, more strict security access policies, and so on. As a result, the CS service usually consumes more cloud resources such as CPU time to compute the complex cryptography algorithms and occupies more hard drive spaces (i.e., strict resource isolation requires that no storage sharing is allowed). Usually, users need to pay more for CS services, which means higher reward to the mobile cloud service provider. To satisfy the security service requirements of end users, i.e., either CS service or NS service, the mobile cloud needs to consider how to *admit mobile users' service requests* to obtain the maximal

978-1-4244-9920-5/11/$26.00 ©2011 IEEE

system reward with the limited cloud resource.

To address the above presented admission issue for security service requests, we propose a Security Service Admission Model (SSAM) based on Semi-Markov Decision Process (SMDP) [4] to leverage the maximal system rewards with the system resource constraints. The contributions of our solutions are two-fold:

- We apply the Semi-Markov Decision Process to analyze the system reward of different security services, and derive the optimal resource allocation policy in the mobile cloud computing.
- We propose SSAM to derive the cloud service blocking probability and achieve the maximum system gain of the mobile cloud by considering both system expenses and incomes (i.e., considering the system reward).

The remainder of this paper is organized as follows. The related work is presented in Section II. In Section III, we present our system models. The Semi-Markov Decision Process model (SMDP) for mobile cloud computing is developed in Section IV. Based on the SMDP model, we derive the blocking probability in Section V. The system performance is evaluated in Section VI, following by concluding remarks and future work in Section VII.

II. Related Work

Recent research has been focused on Cloud computing for mobile devices [5], which enables running applications between resource-constrained devices and Internet-based Clouds. The problem of ensuring the integrity of data storage in Cloud Computing is studied in [6] and [7]. In [8], an economic cloud computing model is presented to decide how to manage the computing tasks with a given configuration of the cloud system. A game theory-based resource allocation model to allocate the cloud resources according to users' QoS requirements is proposed in [9]. Although resource management in wireless networks has been extensively studied in [10], [11], and [12], existing mobile cloud solutions are limited and are solely focused on the enhancement of the individual mobile device's capability. In addition, much of the previous works for cloud security focused on the security to enhance security of Clouds themselves, such as infrastructure security [13], based on TCG/TPM, secure outsourcing [14], and Cloud web security [15], etc. To the best of our knowledge, none of them addressed how to construct a system reward model for resources allocation by considering prioritized cloud security services.

III. System Description

To improve security for cloud computing, two basic security services are provided, namely, NS and CS services. NS service only uses basic security approaches such as authentication to validate the users, and it usually involves low-complexity computing and access control tasks. CS service provides more security services such as confidentiality, digital signature, access control, audition, anti-virus scanning, etc. To simplify the notations, we denote NS and CS services as l and h, respectively.

In our model, the cloud resources are divided into K portions, and each portion represents a VI.

In the cloud, mobile users can choose the desired security services l or h, which occupies α_l VIs and α_h VIs, ($0 < \alpha_l + \alpha_h < K$), respectively. With the limitation of cloud resources (i.e., VIs), it is critical to allocate the resources to maximize the system reward, i.e., leverage the cloud service incomes and system running expenses. In other words, the cloud should decide whether to accept or reject a security service request (l or h) based on the currently available cloud resources and the arrival rate of potential future security service requests.

The arrival rates of security services l and h follow the Poisson distribution with mean rates λ_l and λ_h, respectively. The cloud resource occupation time follows the exponential distribution with mean $1/\mu_l$ and $1/\mu_h$, respectively. In the following, we present the system states, the actions, and the reward model for the presented mobile cloud computing system.

A. System States

An arrival request of security service l or h can be considered as an incoming event, and a departure of a service l or h can be considered as a leaving event. Thus, in the system model, we define three service events: 1) The cloud receives a request of security service l from a user, denoted by e_l; 2) The cloud receives a request of security service h from a user, denoted by e_h; and 3) The transaction of a security service completes and associated VIs are released, denoted by e_f. The number of security service l and security service h being served in the cloud are denoted as N_l and N_h, respectively. Therefore, the system state can be expressed as:

$$\mathcal{S} = \{s | s = \langle \widehat{s}, e \rangle\},$$

where $\widehat{s} = \langle N_l, N_h \rangle$, $e \in \{e_l, e_h, e_f\}$, and $0 \leq \alpha_l N_l + \alpha_h N_h \leq K$.

B. Actions

In system state $\widehat{s}$, upon receiving a service request, (e.g., e_l or e_h), two actions can be selected by the mobile cloud: *accept* and *reject*, which are denoted by $a_{\langle \widehat{s}, e_l/e_h \rangle} = 1$ and $a_{\langle \widehat{s}, e_l/e_h \rangle} = 0$, respectively. When a departure occurs, the cloud releases the cloud resources and there is no action in this case. Thus, we define $a_{\langle \widehat{s}, e_f \rangle} = 0$. Accordingly, the action set is $A = \{a_{\langle \widehat{s}, e \rangle} | a_{\langle \widehat{s}, e \rangle} \in \{0, 1\}\}$.

C. Reward Model

The system net reward can be evaluated based on the service incomes and the running expenses:

$$x(s, a) - \tau(s, a) y(s, a), \tag{1}$$

where $x(s, a)$ is the net lump sum incomes for the cloud when action a is chosen at the current state s, $y(s, a)$ is the service holding cost rate when the cloud is in state s and action a is selected, and $\tau(s, a)$ is the expected service time from the current state s to the next state when decision a is selected. $x(s, a)$ is computed as:

$$x(s, a) = \begin{cases} 0, & a_{\langle \widehat{s}, e \rangle} = 0, \\ R_l, & a_{\langle \widehat{s}, e_l \rangle} = 1, \\ R_h, & a_{\langle \widehat{s}, e_h \rangle} = 1, \end{cases} \tag{2}$$

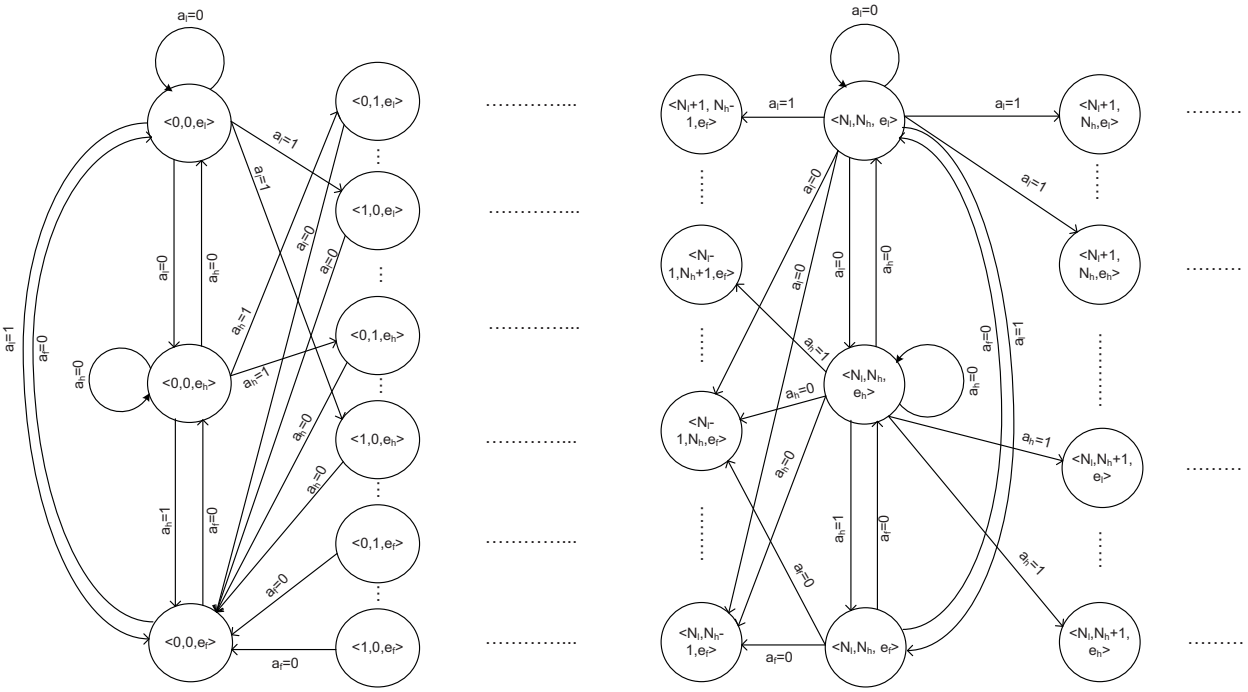

Fig. 2. State transition Diagram.

where R_l and R_h are an income of the cloud when an l and an h security service request is accepted, respectively. The service holding cost rate $y(s,a)$ is proportional to the occupied cloud resources, which is given by

$$y(s,a)=\begin{cases}\alpha_l N_l+\alpha_h N_h, & a_{\langle\widehat{s},e\rangle}=0,\\ \alpha_l(N_l+1)+\alpha_h N_h, & a_{\langle\widehat{s},e_l\rangle}=1,\\ \alpha_l N_l+\alpha_h(N_h+1), & a_{\langle\widehat{s},e_h\rangle}=1.\end{cases} \tag{3}$$

IV. SMDP Based Mobile Computing Model

A general SMDP model consists of six elements [4]: *1) system states; 2) action sets; 3) the events; 4) decision epochs; 5) transition probabilities,* and *6) rewards*. A decision epoch is the time instant when any of the events takes place, e.g., a request of service l or h arrives, or a security service is finished and the allocated resources of VIs are released. The time duration between two decision epoches follows an exponential distribution. Denote $\tau(s,a)$ as the expected time duration between two decision epoches, given the current state s and action a.

Thus, we have

$$\tau(s,a)=\begin{cases}[\gamma+a_{\langle\widehat{s},e_l\rangle}\mu_l]^{-1}, & e=e_l\\ [\gamma+a_{\langle\widehat{s},e_h\rangle}\mu_h]^{-1}, & e=e_h\\ \gamma^{-1}, & e=e_f\end{cases} \tag{4}$$

where $\gamma=\lambda_l+\lambda_h+N_l\mu_l+N_h\mu_h$.

The state transition in a Markov decision model is shown in Fig. 2. Denote $q(j|s,a)$ as the state transition probability from state s to j when action a is chosen. For a state $s=\langle\widehat{s},e\rangle$ where $\widehat{s}=\langle N_l,N_h\rangle$, $e\in\{e_l,e_h,e_f\}$, and action $a=0$, the next state can be $j_1=\langle N_l,N_h,e_l\rangle$, $j_2=\langle N_l,N_h,e_h\rangle$, $j_3=\langle N_l-1,N_h,e_f\rangle$ ($N_1\geq 1$), and $j_4=\langle N_l,N_h-1,e_f\rangle$ ($N_h\geq 1$). $q(j|s,a)$ can be obtained as

$$q(j|s,a)=\begin{cases}\lambda_l\tau(s,a), & j=j_1\\ \lambda_h\tau(s,a), & j=j_2\\ N_l\mu_l\tau(s,a), & j=j_3\\ N_h\mu_h\tau(s,a), & j=j_4\end{cases} \tag{5}$$

Note that $0\leq\alpha_l N_l+\alpha_h N_h\leq K$.

For the current state $s=\langle\widehat{s},e_l\rangle$, and the action $a=1$, the next state can be $j_5=\langle N_l+1,N_h,e_l\rangle$, $j_6=\langle N_l+1,N_h,e_h\rangle$, $j_7=\langle N_l,N_h,e_f\rangle$, and $j_8=\langle N_l+1,N_h-1,e_f\rangle$ ($N_h\geq 1$). Thus, $q(j|s,a)$ can be obtained as:

$$q(j|s,a)=\begin{cases}\lambda_l\tau(s,a), & j=j_5\\ \lambda_h\tau(s,a), & j=j_6\\ (N_l+1)\mu_l\tau(s,a), & j=j_7\\ N_h\mu_h\tau(s,a), & j=j_8\end{cases} \tag{6}$$

Similarly, for state $s=\langle\widehat{s},e_h\rangle$ and action $a=1$, the next state can be $j_9=\langle N_l,N_h+1,e_l\rangle$, $j_{10}=\langle N_l,N_h+1,e_h\rangle$, $j_{11}=\langle N_l-1,N_h+1,e_f\rangle(N_l\geq 1)$, and $j_{12}=\langle N_l,N_h,e_f\rangle$. Thus, $q(j|s,a)$ can be obtained as

$$q(j|s,a)=\begin{cases}\lambda_l\tau(s,a), & j=j_9\\ \lambda_h\tau(s,a), & j=j_{10}\\ N_l\mu_l\tau(s,a), & j=j_{11}\\ (N_h+1)\mu_h\tau(s,a), & j=j_{12}\end{cases} \tag{7}$$

Applying the discounted reward model [4], the expected discounted reward during $\tau(n,a)$ satisfies:

$$\begin{aligned} z(s,a) &= x(s,a)-y(s,a)E_{\widehat{s}}^{a}\left\{\int_0^{\tau_1}e^{-\alpha t}dt\right\}\\ &= x(s,a)-y(s,a)E_{\widehat{s}}^{a}\left\{\frac{[1-e^{-\alpha\tau_1}]}{\alpha}\right\}\\ &= x(s,a)-\frac{y(s,a)\tau(s,a)}{1+\alpha\tau(s,a)}, \end{aligned} \tag{8}$$

where $x(s,a)$ and $y(s,a)$ are defined in (2) and (3). The maximum long term discounted reward is given by

$$\nu(s) = \max_{a \in A} \left\{ z(s,a) + \lambda \sum_{j \in S} q(j|s,a)\nu(j) \right\} \quad (9)$$

where $\lambda = (1 + \alpha\tau(s,a))^{-1}$. Let w be a finite constant, $w = \lambda_l + \lambda_h + K * \max(\mu_l, \mu_h) < \infty$, and $\tilde{\lambda} = w/(w+\alpha)$. The optimality equation of $\nu(s)$ can be obtained after uniformization,

$$\tilde{\nu}(s) = \max_{a \in \tilde{A}} \left\{ \tilde{z}(s,a) + \tilde{\lambda} \sum_{j \in \mathcal{S}} \tilde{q}(j|s,a)\tilde{\nu}(j) \right\} \quad (10)$$

where $\tilde{z}(s,a) \equiv z(s,a)\frac{1+\alpha\tau(s,a)}{(\alpha+w)\tau(s,a)}$, and

$$\tilde{q}(j|s,a) = \begin{cases} 1 - \frac{[1-q(s|s,a)]}{\tau(s,a)w}, & j = s \\ \frac{q(j|s,a)}{\tau(s,a)w}, & j \neq s. \end{cases} \quad (11)$$

V. Blocking Probability

The blocking probability is an important QoS metric for a mobile cloud system. In this section, we derive the blocking probability using the proposed SMDP-based SSAM.

The expected total discounted reward $\tilde{\nu}(s)$ at state $s \in \mathcal{S}$ is dependent on $\lambda_l, \lambda_h, \mu_l, \mu_h$ and K, as shown in (10). Our objective is to find a decision rule that maximizes the total reward at each state, $\tilde{\nu}(s)$, $\forall s$. In specific, when a security service request arrives, the system resource management model checks $\tilde{\nu}(s)$ of the current state under different actions, i.e., $a = 0$, or $a = 1$, and select an action with a higher reward.

We derive the steady state probability, denoted as $\pi_{\langle N_l, N_h, e\rangle}$ for state $\langle N_l, N_h, e\rangle$ in SSAM as shown in Fig. 2. We use states $(j_1, .. j_{12})$ defined in Section IV to simplify the notation. Similarly, let $j_{13} = \langle N_l, N_h - 1, e_h\rangle (N_h \geq 1)$, $j_{14} = \langle N_l - 1, N_h, e_l\rangle (N_l \geq 1)$.

The stead state probability of $\pi_{\langle N_l, N_h, e\rangle}$ can be derived as follows

$$\pi_{j_1} = \begin{cases} (1-a_{j_1})\pi_{j_1}\frac{w+\lambda_l-\beta}{w} + (1-a_{j_2})\pi_{j_2}\frac{\lambda_l}{w} & N_l = 0, N_h = 0 \\ \quad + a_{j_1}\pi_{j_1}\frac{w-\beta-\mu_l}{w} + \pi_{j_7}\frac{\lambda_l}{w}, & \\ (1-a_{j_1})\pi_{j_1}\frac{w+\lambda_l-\beta}{w} + (1-a_{j_2})\pi_{j_2}\frac{\lambda_l}{w} & N_l = 0, N_h > 0 \\ \quad + a_{j_1}\pi_{j_1}\frac{w-\beta-\mu_l}{w} + \pi_{j_7}\frac{\lambda_l}{w} + a_{j_{13}}\pi_{j_{13}}\frac{\lambda_l}{w}, & \\ (1-a_{j_1})\pi_{j_1}\frac{w+\lambda_l-\beta}{w} + (1-a_{j_2})\pi_{j_2}\frac{\lambda_l}{w} & N_l > 0, N_h = 0 \\ \quad + a_{j_1}\pi_{j_1}\frac{w-\beta-\mu_l}{w} + \pi_{j_7}\frac{\lambda_l}{w} + a_{j_{14}}\pi_{j_{14}}\frac{\lambda_l}{w}, & \\ (1-a_{j_1})\pi_{j_1}\frac{w+\lambda_l-\beta}{w} + (1-a_{j_2})\pi_{j_2} & \\ \quad + a_{j_1}\pi_{j_1}\frac{w-\beta-\mu_l}{w} + \pi_{j_7}\frac{\lambda_l}{w} & N_l > 0, N_h > 0 \\ \quad + a_{j_{13}}\pi_{j_{13}}\frac{\lambda_l}{w} + a_{j_{14}}\pi_{j_{14}}\frac{\lambda_l}{w}, & \end{cases} \quad (12)$$

$$\pi_{j_2} = \begin{cases} (1-a_{j_1})\pi_{j_1}\frac{\lambda_h}{w} + (1-a_{j_2})\pi_{j_2}\frac{w+\lambda_h-\beta}{w} & N_l = 0, N_h = 0 \\ \quad + a_{j_2}\pi_{j_2}\frac{w-\beta-\mu_h}{w} + \pi_{j_7}\frac{\lambda_h}{w}, & \\ (1-a_{j_1})\pi_{j_1}\frac{\lambda_h}{w} + (1-a_{j_2})\pi_{j_2}\frac{w+\lambda_h-\beta}{w} & N_l = 0, N_h > 0 \\ \quad + a_{j_2}\pi_{j_2}\frac{w-\beta-\mu_h}{w} + \pi_{j_7}\frac{\lambda_h}{w} + a_{j_{13}}\pi_{j_{13}}\frac{\lambda_h}{w}, & \\ (1-a_{j_1})\pi_{j_1}\frac{\lambda_h}{w} + (1-a_{j_2})\pi_{j_2}\frac{w+\lambda_h-\beta}{w} & N_l > 0, N_h = 0 \\ \quad + a_{j_2}\pi_{j_2}\frac{w-\beta-\mu_h}{w} + \pi_{j_7}\frac{\lambda_h}{w} + a_{j_{14}}\pi_{j_{14}}\frac{\lambda_h}{w}, & \\ (1-a_{j_1})\pi_{j_1}\frac{\lambda_h}{w} + (1-a_{j_2})\pi_{j_2}\frac{w+\lambda_h-\beta}{w} & \\ \quad + a_{j_2}\pi_{j_2}\frac{w-\beta-\mu_h}{w} + \pi_{j_7}\frac{\lambda_h}{w} & N_l > 0, N_h > 0 \\ \quad + a_{j_{13}}\pi_{j_{13}}\frac{\lambda_h}{w} + a_{j_{14}}\pi_{j_{14}}\frac{\lambda_h}{w}, & \end{cases} \quad (13)$$

where $\beta = N_l\mu_l + N_h\mu_h + \lambda_l + \lambda_h$, $0 \leq \alpha_l N_l + \alpha_h N_h \leq K$.

As the total probability equals to 1, we have

$$\sum_{N_l}\sum_{N_h} \pi_{\langle N_l, N_h, e\rangle} = 1. \quad (14)$$

Solving Eq. (12 - 14), the steady-state probability $\pi_{\langle N_l, N_h, e\rangle}$ can be iteratively obtained. The blocking probability $P_{blocking}$, defined as the ratio of the number of rejected requests and the total number of service requests, is thus given by

$$P_{blocking} = \frac{\sum_{N_l}\sum_{N_h}\left((1-a_{j_1})\pi_{j_1} + (1-a_{j_2})\pi_{j_2}\right)}{\sum_{N_l}\sum_{N_h}\left(\pi_{j_1} + \pi_{j_2}\right)}, \quad \text{for } \alpha_l N_l + \alpha_h N_h \leq K, \quad (15)$$

where $a_{j_1}, a_{j_2} \in A$ are the actions adopted at states $\langle N_l, N_h, e_l\rangle$ and $\langle N_l, N_h, e_h\rangle$, respectively.

VI. Performance Evaluation

In this section, we evaluate the performance of the proposed SSAM using a simulator written in matlab. We set up a cloud system with the total number of VIs from 2 to 15. The request arrival rates of services l and h are 5 and 2 per unit time, respectively, and the average service holding time of each connection is $\mu_l = \mu_h = 6$ unit times, if not otherwise specified. A service h occupies two VIs while l occupies one VI when it is accepted. Accordingly, an income of 0.3 for l and 0.6 for h are added to the cloud system. We set the discount factor $\alpha = 0.1$ to assure the convergence of the reward computation.

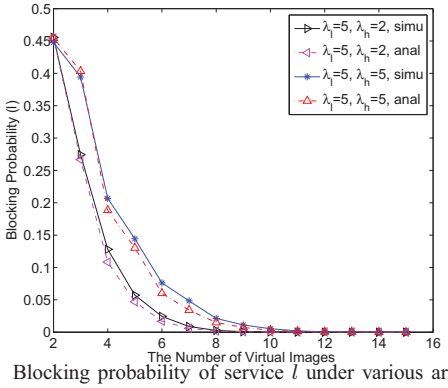

Fig. 3. Blocking probability of service l under various arrival rates.

The blocking probabilities of services l and h under various arrival rates of service requests are shown in Fig. 3 and Fig. 4, respectively. A lower blocking probability is achieved when more network resources, e.g., VIs, are available. Because service h requires two times cloud resources than service l,

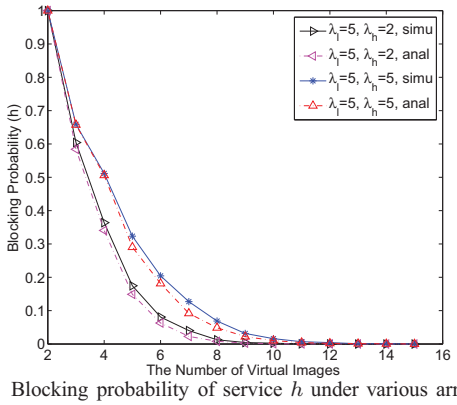

Fig. 4. Blocking probability of service h under various arrival rates.

h is more likely to be rejected, especially when the cloud resource is limited, e.g., only two VIs in the cloud. Therefore, the blocking probability of service h is larger than that of service l accordingly. We further increase the arrival rate of service h from 2 to 5 per unit time. It can be seen that the blocking probability increases with the traffic arrival rates for a given the network resource.

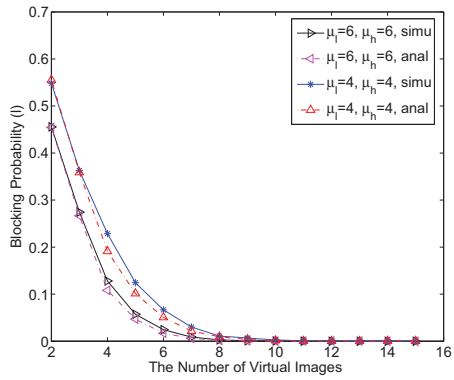

Fig. 5. Blocking probability of service l under various service occupation times.

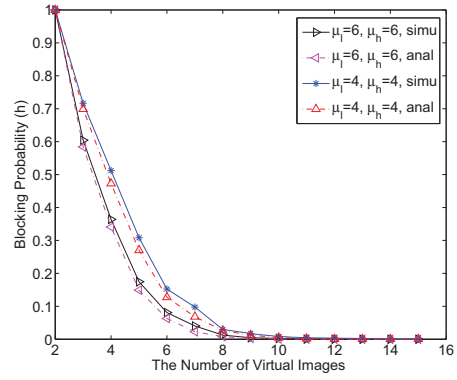

Fig. 6. Blocking probability of service h under various service occupation times.

The blocking probabilities of different services under various service departure rates are shown in Fig. 5 and Fig. 6. With a larger service holding time, the system cost of each mobile user increases, which results in a degraded system reward. Therefore, a new request is more likely to be rejected. The blocking probability decreases with the service occupation time for both services l and h.

VII. Conclusion

In this paper, we have proposed a SSAM based on SMDP considering both the maximal system reward and system service expenses. The system reward is derived through SSAM by taking into considerations of the CS/NS service rewards and their cloud system expenses. We derive the blocking probabilities of SSAM and conduct extensive simulations to validate our analysis. In the future, we will investigate the optimal system resources (i.e., the number of VIs) to obtain the maximal system rewards under the given blocking probability. In addition, we will incorporate more system metrics into the constructions of the reward function such as different application tasks as well.

Acknowledgment

Hongbin Liang's research is supported by the China Scholarship Council and Dijiang Huang's research is sponsored by ONR YIP award.

References

[1] D. Huang, X. Zhang, M. Kang, and J. Luo, "Mobicloud: A secure mobile cloud framework for pervasive mobile computing and communication," in *Proceedings of 5th IEEE International Symposium on Service-Oriented System Engineering*, 2010.

[2] H. Raj, R. Nathuji, A. Singh, and P. England, "Resource management for isolation enhanced cloud services," in *Proceedings of ACM workshop on Cloud computing security*, 2009, pp. 77–84.

[3] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," in *ACM Conference on Computer and Communications Security*, 2009.

[4] M. Puterman, *Markov decision processes: Discrete stochastic dynamic programming*. John Wiley & Sons, Inc. New York, NY, USA, 2005.

[5] X. H. Li, H. Zhang, and Y. F. Zhang, "Deploying Mobile Computation in Cloud Service," in *Proceedings of the First International Conference for Cloud Computing (CloudCom)*, 2009, p. 301.

[6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in *European Symposium on Research in Computer Security (ESORICS) 2009*, Saint Malo, France, Sep 2009.

[7] C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditably Secure Data Storage Services," *IEEE Network Magazine*, vol. 24, no. 4, pp. 19–24, July/August 2010.

[8] H. Liang, D. Huang, and D. Peng, "On Economic Mobile Cloud Computing Model," in *Proceedings of the International Workshop on Mobile Computing and Clouds (MobiCloud in conjunction with MobiCASE)*, 2010.

[9] G. Wei, A. V. Vasilakos, Y. Zheng, and N. Xiong, "A game-theoretic method of fair resource allocation for cloud computing services," *The Journal of Supercomputing*, vol. 54, no. 2, pp. 252–269, 2009.

[10] L. X. Cai, L. Cai, X. Shen, and J. W. Mark, "Resource management and QoS provisioning for IPTV over mmWave-based WPANs with directional antenna," *ACM Mobile Networks and Applications (MONET)*, vol. 14, no. 2, pp. 210–219, 2009.

[11] H. T. Cheng and W. Zhuang, "Novel packet-level resource allocation with effective QoS provisioning for wireless mesh networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 2, pp. 694–700, Feb 2009.

[12] L. X. Cai, X. Shen, and J. W. Mark, "Efficient MAC Protocol for Ultra-wideband Networks," *IEEE Communications Magazine*, vol. 47, no. 6, pp. 179–185, 2009.

[13] N. Santos, K. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," in *Proceedings of USENIX HotCloud*, 2009.

[14] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," in *Proceedings of the 2009 ACM workshop on Cloud computing security*, 2009, pp. 85–90.

[15] J. Sobey, T. Whalen, R. Biddle, P. V. Oorschot, and A. Patrick, "Browser Interfaces and Extended Validation SSL Certificates: An Empirical Study," in *Proceedings of the 2009 ACM workshop on Cloud computing security*, 2009.