Security Analysis of Cloud Computing in the Mobile Internet Environment

LUOMINGWAN[1, a]

[1]Yangjiang Vocational and Technical College, Yangjiang Guangdong,China,529500

[a]85949463@qq.com

Keywords: Cloud computing, Cloud access control, Mobile Internet, Optimized decision

Abstract. In order to improve the benefits of the mobile cloud computing network and the quality of the security service of the mobile cloud computing, this paper aims to make a design of the control framework of the cloud computing resources of the cloud computing security service among its service domains, and design the optimal decision-making strategy of the allocation and management of the resources. The system, which combines the design of the decision mechanism of the access control, the analysis of the energy consumption and response time in view of the task execution, and the selection of the optimal access path, makes it possible for high security and low energy consumption.

Introduction

Due to the unique advantages of cloud computing and huge business prospects, many companies in the field of mobile Internet have provided or ready to provide a variety of cloud computing services combined with their own industry[1, 2, 3]. Due to the introduction of cloud computing into mobile Internet, changes and new security challenges will be brought about. In order to solve the security problem, it is necessary to systematically study the security risk of the mobile Internet, and build security technology system for cloud computing.

According to the requirement of document protection in mobile Internet,a new access control scheme based on attribute encryption (CP-ABE) is designed by setting up a small cloud computing platform and building up a cloud security framework. According to the scheme, lightweight devices can safely utilize the computing resources provided by the cloud service provider to outsource the encryption/ decryption of the cloud computing, without the worry of exposing the sensitive data of the terminals. The advantages of the proposed scheme in terms of the security, storage and computation are verified through the performance evaluation, and the mallicious attacking samples are also tested. The evaluation results are analyzed in this paper to verify the effectiveness and accuracy of the scheme.

The cloud security framework of the Mobile Internet

As the core and the trend of the development of the Internet in the future, the mobile Internet has put forward a new challenge to security research with the increase of related mobile applications and the expansion of interconnection and openness. Mobile internet security policy will be based on the architecture of the mobile Internet, business requirements, security threats and the analysis results of security needs, while mobile Internet protection architecture is based on the principle of the division of system security domain, covering the overall security architecture, which includes the infrastructure, network services, and business applications. The overall mobile Internet protection strategy mainly includes the automatic audit of the mobile Internet Security Strategy, the illegal invasion strategy, the business security strategy, and the false accounting security policy. According to the end to end secure communication standards, based on the mobile Internet architecture, business requirements, security threats and security requirements analysis results, the overall mobile Internet security framework, the overlaid infrastructure, netword services and business applications are proposed. As shown in figure 1.

© 2016. The authors - Published by Atlantis Press

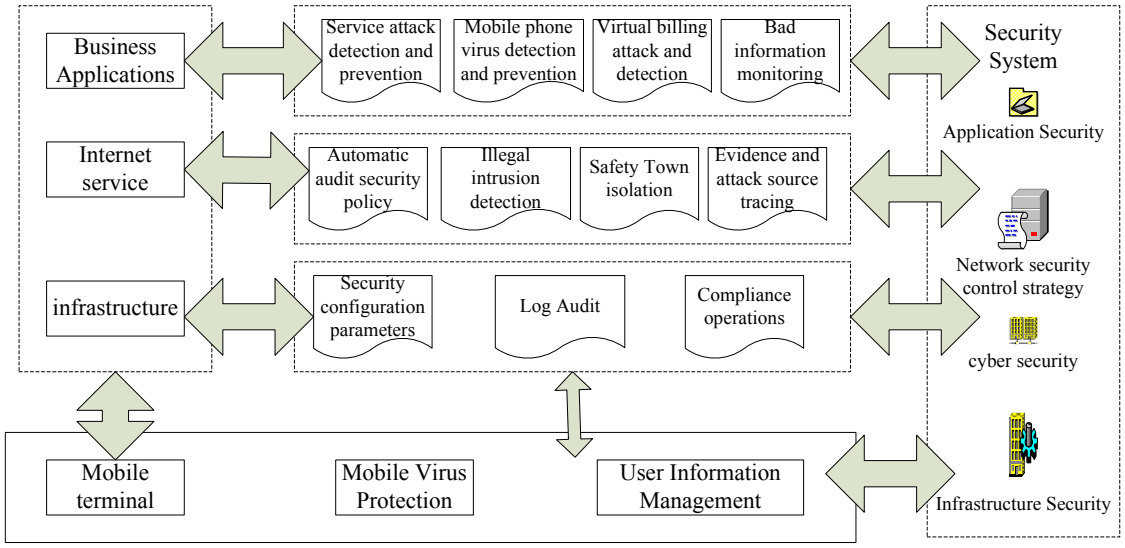

Figure 1 The overall mobile Internet protection framework

The security threats in mobile Internet exist in all aspects,including terminal security, network security and business security threats etc. The emergence and popularity of intelligent terminals has brought potential threats, such as illegal tampering and illegal access to information, the use of the operating system to modify the relevant terminal information, and the use of the virus and malicious code to destroy the system. Data transmission through wireless channel is easily intercepted or illegally tampered, and thus difficult to protect the confidentiality and integrity of the data.

Design of security service model for mobile cloud computing

The number of available VM in the mobile cloud computing service domain must be updated accordingly. The cloud computing security service used to represent C VM cloud computing resources leaves the mobile cloud computing services domain, of which $1 \le c \le C$. Thus the event and its collection in the mobile cloud computing service domain can be represented as $e \in \{A_1, A_2, \Lambda\ , F_1, \Lambda\ F_C\}$. The completion of the operation of the cloud computing security services to leave the mobile cloud computing service domain can be expressed in the formula as:

$$S = \{s \mid s =< s_1, s_2, \Lambda\ , s_C, e >=< \bar{s}, e >\} \quad (1)$$

$$\bar{s} =< s_1, s_2, \Lambda\ , s_C > \quad (2)$$

$$\sum_{c=1}^{C} (s_c * c) \le K \quad (3)$$

Three kinds of actions can be selected from the action set in the mobile cloud computing service domain, they are: 1)receiving the request from the cloud computing security services and allocating C VM cloud computing resources to the cloud computing security services;2)refusing the request of the cloud computing security service; 3)or transferring the request to the neighboring mobile cloud computing services domain for operation, which can be expressed as $a(s) = c, c =\in \{1,2,\Lambda\ , c\}, a(s) = 0, a(s) = 1$. When a cloud computing security services end its operation, it will release the cloud computing resources. The system action is to update the cloud computing resources available in the mobile cloud computing service domain (i.e., updating the number of available VM), which can be expressed as $a(s) = -2$. The action space of the mobile cloud computing resource management model is Acts={-2, -1, 0,1,2,..., C}. Thus the action set of a(s) can be expressed as:

$$a(s) = \begin{cases} \{-1,0,1,\Lambda\ , C\} & e \in \{A_n, A_t\} \\ -2 & e \in \{F_1, F_2, \Lambda\ , F_C\} \end{cases} \quad (4)$$

The system state and the corresponding actions based on the resource management model of the mobile cloud computing security services, and the overall system revenue of the mobile cloud computing network can be expressed as:

$$r(s,a) = w(s,a) - g(s,a) \qquad (4)$$

$$w(s,a) = \begin{cases} 0 & a(s=-2, e \in \{F_1, \Lambda\ , F_C\} \\ E_d - E_t - \delta_s\beta - \delta_d\beta & a(s) = -1, e = A_n \\ -\delta_s\beta - \delta_d\beta & a(s) = -1, e = A_t \\ -U_d - \theta_d\beta & a(s) = 0, e = A_n \\ 0 & a(s) = 0, e = A_t \\ E_d - \delta_d\beta - \beta / cu & a(s) = c, e = A_n \\ E_t - \beta / cu & a(s) = c, e = A_t \end{cases} \qquad (5)$$

In the formula of $s = (\bar{s}, e), e \in \{A_n, A_t, F_1, \Lambda\ , F_C\}.w(s,a)$, S is the system state of the mobile cloud computing network. When an event E happens, S is the system revenue after the corresponding decision A is made. G (s, a) is expected system overhead for mobile cloud computing networks, and the expected system costs of the resource management model can be expressed as:

$$g(s,a) = \tau(s,a)o(s,a), a(s) \cup Act_s \qquad (6)$$

When the current system state is H and the decision selected is A, τ (s, a) represents the expected time needed for the transfer of the system to the next state; and all of the cloud computing resources occupied by the running security services in the domain(expressed by VM). It represents the costs needed for occupying the the cloud computing resources by the running cloud computing security services which are calculated by unit time. It shares the same measurement unit with the revenue from the mobile cloud computing service domain, and can be expressed in the formula as:

$$o(s,a) = \sum_{c=1}^{C} (s_c * c) \qquad (7)$$

When the system state of mobile cloud computing network is S, if the decision taken by the system is a, we use τ (a, s) to represent the time from the current decision point to the next decision point. Therefore, when the system state and the decision selected under it are established, the average rate (used to express) for any events taking place in the mobile cloud computing network is the sum of the mean rate for all events in the networks (because the occurrance of all events in the mobile cloud computing network obeys Poisson distribution), which can be expressed as,

$$\Gamma(s,a) = \tau(s,a)^{-1} = \begin{cases} \lambda_n + \lambda_t + \sum_{c=1}^{C} s_c cu & e \in \{F_1, \Lambda\ , F_C\}, e \in \{A_n, A_t\}, a = 1 \,\&\, a = 0 \\ \lambda_n + \lambda_t + \sum_{c=1}^{C} s_c cu + cu & e \in \{A_n, A_t\}, a = c \end{cases} \qquad (8)$$

Security strategy analysis of mobile cloud computing

MCC access control model and architecture

According to the study of the key technology of mobile access control mechanism in MCC, the traditional cloud access control system based on attribute encryption (ABE) is focused on the division of encryption / decryption. The task is about how to split an access control system into the cloud or to introduce locally a network with a new view. At this time, besides the consideration of the parameters of bandwidth and delay, two different types of wireless networks should also be considered: Wi-Fi IEEE802.il networks and mobile cellular networks, such as 3G or LTE networks. In the framework of MCC, a interface layer of a mobile device and the corresponding cloud is introduced, known as cloudlet access layer, and is deployed at the Wi-H hot near the device. The access control

infrastructure based on MCC proposed according to the scheme is made for cloud service provider, not for network provider/operator. At present, most of the literatures focus on the division of the access control , and the mechanism proposed in this chapter will focus on the localization problem based on cloudlet. The MCC access control system is characterized by supporting two layers: mobile cloud and access to the cloudlet layer. The current mainstream access control framework fails to support the two layers, as shown in Figure 3.

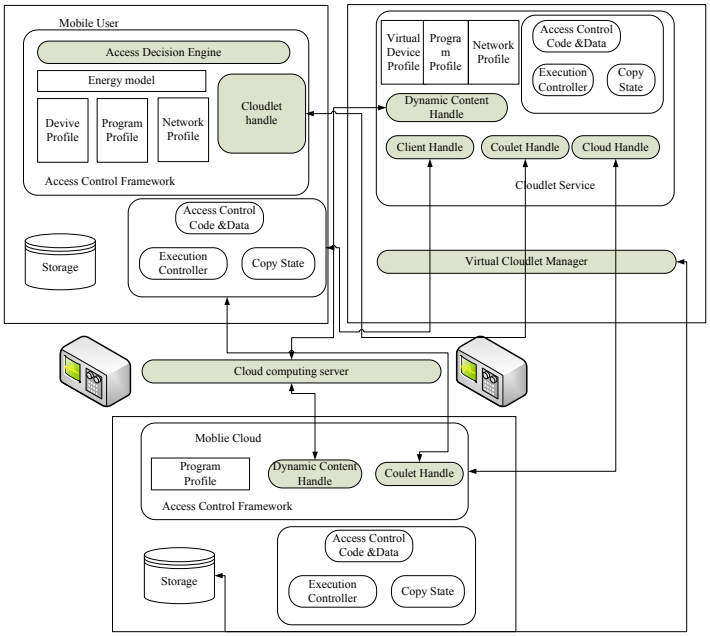

Figure 2 MCC access control architecture

Mobile cloud is made up of public cloud service providers with large amounts of cloud server, and provides corresponding virtual machine for mobile devices, where internal communication can be made possible among virtual machines, which is similar to Cloudlets. A single Cloudlet can be seen as a kind of virtual machine with abundant resources, when it is connected to the nest base station by installing the access point, it plays a role in the access cloud, and helps to realize the internal connection to the transmission of the user's data.

The algorithm design of the mobile network security control

First, a randomized polynomial time algorithm is used to define the scheme:

（1）$Step(K,m,n) \to \{params, MK_0\}$, a safety parameter ruler is selected,with m for the attribute and n for users, both used as input. The output system parameter of TTP is params and the master key is MK_0. The system parameter is for the attribute set U={1, 2, ..., m} and for the User identity set I = {1, 2, …, n}.

（2） $GreatUse(\text{params}, \text{MK}_0, \omega, \text{ID}) \to (SK_{ID,\omega})$. DM first check for Γ to see if the user is qualified, that is $\omega \in U, ID \in I$. If it is qualified, then arams and master key are used, as a result, an user master key is generated, otherwise it outputs “NULL”.

（3）$\text{Encrypt}(\text{params}, \Gamma, \text{f}) \to (CT)$ If the user selects f to visit control Γ , and params as the input, then the output is a ciphertext CT.

（4） $\text{Decryp}(\text{params}, SK_{\text{ID},\omega}, \text{CT}) \to (f)$ Users who meet the attribute set $\omega^1 \in \{i \mid \omega \cap \overline{\Gamma}\}$ choose paramas, with ciphertext and user’s private key as input, and plaintext is restored.

In the encryption process, firstly mobile users run the access decision mechanism of Access Decision Engine to make a choice of the access path, and at the same time, is connected to the nearest cloudlet by utlizing Cloudlet hander module. If the choice of calculated path cloudlet is the optimal,CT is sent to the client handle module in the cloudlet layer through Wi-Fi network, and is uploaded to the cloud through Dynamic Content Handle. In this way, the flow of mobile users can be

saved for not using the service provided by the network operators. When connected to the cloud Storage module, cloudlets can use Dynamic Content Handle to download CT immediately through the cloud and the fixed network of cloudlet layer. Finally it returns to the desired value to the mobile user's Execution Controller recovery. Throughout the process, the virtual machine in the cloudlets bears a heavy computing task, and its function is similar to the cloud services.

According to the scheme, the majority of the revocation of the computing tasks is handled by the CSP through the cloud services resources,and the relevant security is defined as follows.

（1） Re - encryp(params, $(A_{l\times k}, \rho)$, $\{R_{\rho(x)}\}_{x\in\{1,2,\Lambda,l\}}$, f)： CSP randomly chooses $\eta_x^{'}, s_x^{'} \in Z_N$, the formula is:

$$C_{x,2} = g^{\eta_x^1}(h_{\rho_{(x)}}\prod_{j\in I} g_{n+1-j})^{\lambda_x} \quad (9)$$

$$C_{x,3} = g^{\eta_x^1} \quad (10)$$

$$C_{x,4} = g^{\eta_x^1}(\prod_{j\in R_{\rho(x)}} g_{n+1-j})^{s_x^{'}} \quad (11)$$

The new ciphertext is:

$$CT = (C_0, C_1, \{C_{x,0}, C_{x,1}, C_{x,3}, C_{x,4}, R_{\rho(x)}\}_{x\in\{1,2,\Lambda,l\}}) \quad (12)$$

（2） Re - decrypt : firstly, $L = \{x \mid \rho(x) \in \omega, ID \notin R_{\rho(x)}\}$, so $\omega^{'} = \{\rho(x)\}_{x\in L}$, if the user's $\omega^{'}$ meets the access structure $(A_{i\times k}, \rho)$, for and $x \in L$, the formula is:

$$D_x = \frac{\bar{e}(K_{\rho_{(x),1}}, C_{x,0})}{(K_{\rho_{(x),2}}, C_{x,1})} \cdot \frac{\bar{e}(C_{x,0}, \prod_{j\in i, j\neq ID} g_{n+1-J+ID})}{\bar{e}(g_{ID}, C_{x,2})} \cdot \frac{\bar{e}(g_{ID}, C_{x,4})}{\bar{e}(C_{x,3}, \prod_{j\in R_{\rho(x)}} g_{n+1-J+ID})} = \frac{\bar{e}(g^{a-t}, g^{\lambda_x})}{\bar{e}(g_1, g_n)^{\lambda_x}} \quad (13)$$

If Ux is the recovery factor in the X line,the user can successfully recover the file f:

$$C_o \frac{1}{\bar{e}(K_o, C_1)} \cdot \prod_{x\in L} D_x^{u_x} = f \cdot \bar{e}(g_1, g_n)^s \cdot \frac{1}{\bar{e}(g^t, g^{a-s})} \cdot \frac{\bar{e}(g^{a-t}, g^{\sum_{x\in L}\lambda_{x\mu_x}})}{\bar{e}(g_1, g_n)^{\sum_{x\in L}\lambda_{x\mu_x}}} = f \quad (14)$$

During decryption,because the core value $\bar{e}(g^{a-t}, g^{\lambda_x})$ of recovering F is bound to the user's private key, so, when the mobile user sends $\bar{e}(g^{a-t}, g^{\sum_{x\in L}\lambda_{x\mu_x}})$ to the cloudlets, it is safe to use the VirtualCloudlet Manager of the cloudlet layer to calculate the value. In addition, cloudlet can download code cache from the cloud Storage to improve computing efficiency.

Evaluation of the system model

The event trigger simulation software written by Matlab is used to evaluate the performance of the security service resource allocation and management model, all the experimental results satisfy confidence interval with confidence level of 95%, and the error range is less than 1%. Other parameters used are shown in Table 1.

Table 1 simulation parameters table

Parameter	E_d	E_t	δ_d	δ_s	U_d	θ_d	β
Value	50	80	30	3	10	60	1

Assuming that the network state of each access instance is constant, such as bandwidth and network latency, the CPU performance is one million per second(MIPS); Assuming that the cloud server CPU (MIPS) is two times the CUP of the mobile device, it can also be adjusted accordingly. That is, if the speed of selection for the mobile device is set to 500MIPS, the CPU of the cloud and the cloudlet is 1000 MIPS. Assuming that the maximum bandwidth of the wireless network in the Cloudlet+Cloud structure is 300 Mbit/s (802.11 n wireless devices can be set for higher bandwidth). The traditional access framework of Cloud Only is set to 15 Mbit/s for bandwidth, and the delay for

0.020s(based on the average latency generated by mobile devices in the 3G or Wi-n network). In Figure 4 and Figure 3,the packet loss ratio of the transfer service request and the new service request in the the mobile cloud computing security service resource management optimization model is compared with that of GreedyAlgorithm. For the greedy algorithm, as long as there are enough cloud computing resources in the system, greedy algorithm will allocate as much as possible the VM cloud computing resources to the cloud computing security service request to obtain the highest instant income without considering the long-term gains.

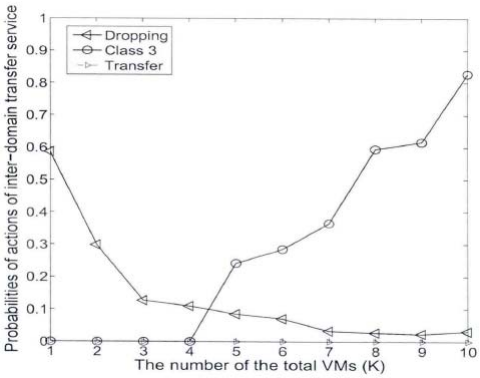

Fig. 3 Decision probability of transferring service request

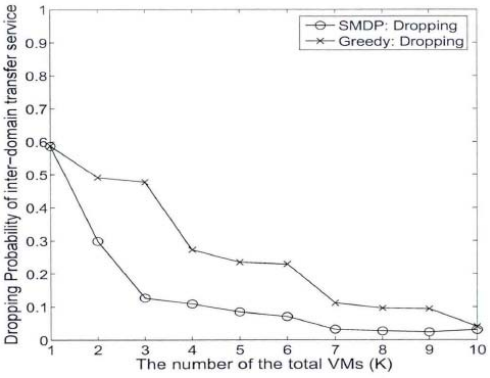

Fig. 4 Packet loss rate of transferring service request

As shown in Figure 5,when the wireless bandwidth is reduced to a certain number,and when the access task and the input data are same, there will be changes to the response time. Traditional access structure can only rely on the bandwidth provided by the wireless network operators, while the access architecture proposed in this chapter provides diverse network bandwidth service, namely Cloudlet based on Wi Fi and the fixed network connected to the Clound.

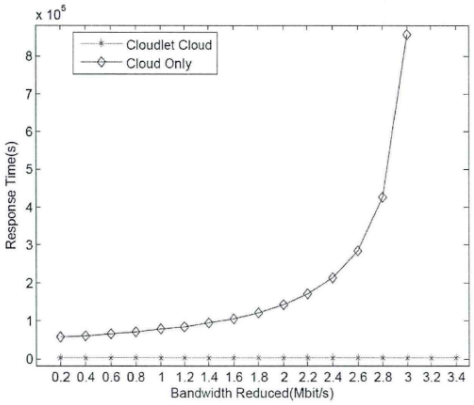

Fig. 5 Schematic diagram of wireless bandwidth and response time

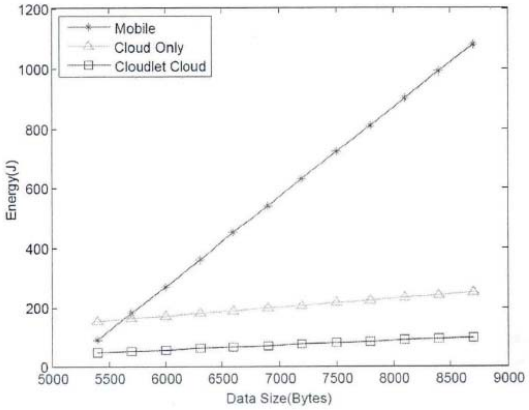

Fig. 6 Schematic diagram of input data and energy consumption

Figure 6 compares the energy consumption of the encryption task (which can be encryption or decryption in the real situation) in different situations, including only on mobile devices and in the case of CloudOnly or Cloudlet+Cloud. When the input data is increased for the same task, Cloudlet+Cloud can save a lot of energy due to its high bandwidth and low delay system structure, and the energy consumption is also reduced for reducing the transmission of data compared to the traditional network structure in access control.

Conclusion

In this paper, the concept of virtual machine (VM) is used to represent the unit computing resources managed by each mobile cloud computing service domain. In the practical research, the resources of mobile cloud computing can also be expressed by the number of server cluster in the mobile cloud computing service domain. The performance of mobile cloud computing network is greatly improved for mobile cloud computing service providers and mobile cloud computing users. The cloudlet layer is added between the mobile device and the traditional cloud infrastructure. When

cloudlets is deployed in the vicinity of the AP with the Wi-Fi, and used as localization services near the mobile device, the response time is effectively reduced, and the performance is improved. The two purposes are achieved when access control algorithm is used in the system to decide the MCC access path, namely minimizing the service response time and the optimal energy consumption of mobile device. Finally the user's experience for the mobile device is effectively enhanced.

References

[1] A Armando,D Basin, Y Boichut, The AVI SPA Tool for the Automated Validation of Internet Security Protocols and Applications[J],Lecture Notes in Computer Science, 2005, Volume 3576/2005, PP 135-165.

[2] Mun Choon Chan, Ramjee R, Improving TCP/IP Performance over Third-Generation WirelessNetworks [J], Mobile Computing, IEEE Transactions on, Volume 7, Issue 4,PP 430-443.

[3]Zhou Gongye, Yi Kai, Chen Jincai, Object storage security authentication mechanism based on role access control. Design of Computer Engineering,Vol 24, 2007,p 5847-5849.

[4] Younchan Jung, Peradilla M, Tunnel gateway satisfying mobility and security requirements of mobile and IP-based networks[J],IEEE Journal of Communications and Networks, 2011, Volume 13, Issue 6, PP583 - 590.

[5]Liu Side. Analysis and discussion of cloud storage model based on network.Science and Technology Bulletin,Vol 28,2012,28,p206-209.

[6]Xiao Long, Zhang Cui, Lu Kaining, The improved design based on trend and Rising Cloud Security. Chinese Education Network, Vol 02,2011,p86-87.

[7] KhanA. R.,Othman M,,Madani S. A. and Khan S. U.,"A Survey of Mobile Cloud Computing Application Models", lEEECommunications Surveys &Tutorials, vol. 16, no.l, 2014,pp.393-413.

[8] LanZ., Varadharajan V. and Kitchens M" "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage",IEEE Transactions onlnformation Forensics and Security, vol.8,no,12, 2013, pp. 1947-1960.

[9] C. J. Martinez, D. K. Pandya,and W.-M. Lin, "On designing fast nonuniformly distributed ip address lookup hashing algorithms,,,IEEE/ACM Trans. Netw., 2009,vol. 17,no. 6,pp. 1916-1925