International Journal of u- and e- Service, Science and Technology
Vol.8, No.4 (2015), pp.1-8
http://dx.doi.org/10.14257/ijunesst.2015.8.4.01

An Access Control Model for Mobile Networks based on the Non-zero-sum Game Theory

Yi-xuan Zhang[1,a], Jing-sha He[1,2,b] and Ruo-hong Liu[2,c]

[1]*School of Software Engineering, Beijing University of Technology, Beijing 100124, China*
[2]*Beijing Development Area Co., Ltd., Beijing 100176, China*
[a]*S201125006@emails.bjut.edu.cn,* [b]*jhe@bjut.edu.cn,* [c]*lrh450820@126.com*

Abstract

Access control is the basic of information security. It is always used to protect sensitive information and critical resources from malicious attacks. But the traditional access control models are more adapt to closed network environment. And there are more and more unknown threats and attacks in the open networks, especially the mobile networks. To solve this problem, we propose a new access control model which is applicable to the open mobile networks by using non-zero-sum game theory in this paper. The model is composed by six modules: access evaluation module, access permission determination module, non-zero-sum game theory analysis module, decision-making module, result evaluation module, access feedback module and a prior information database. And in this model, the subjects will choose to be more honest when they make access requests because they all want to get more permission next time. Then we do some experiments to prove this fact.

Keywords: *access control; mobile networks; non-zero-sum game theory; Nash equilibrium*

1. Introduction

Access control, which is used to protect the critical information and sensitive data from being attacked and threaten, has been an important technology in information security. But traditional access control models are more suitable to relatively static networks environment which is centralized. In this environment, the participants are all we known, and these models could punish malicious access requestors by the punishment mechanism outside the networks punishment. But the mobile networks environment is quite different from the static network environment. In the mobile networks, the number and the exact identity of the participants are always changing dynamically most of the time. And there is no control center to management all resources and data, the service providers distributes scattered in the mobile networks. So the traditional access control models are not suitable to the mobile networks. There need a new access control model which should be dynamically adapt to environment which is always changing.

Non-zero-sum game theory is a typical game theory to solve many problems in biology, economics, computer science, political science, military strategy, and many other disciplines [1]. In non-zero-sum game, the sum of what each player gets or losses is not zero. It means that what one player gets is not equal to what the others losses. Namely, one player could not get gains by harming other players' interests. Therefore, the players in the non-zero-sum game could all choose cooperative strategies and get good benefit. This status is called Nash equilibrium [2]. So we use non-zero-sum game theory to establish an access control model open to mobile

ISSN: 2005-4246 IJUNESST

networks. Access control then has the capability of regulating incoming access requests to effectively curb malicious access in mobile systems and networks. In this model, the players in the game are subject who proposes access requests and object who responses these requests. We build a mechanism to deal with the threats and attacks in mobile networks by seeking for the Nash equilibrium.

The rest of this paper is organized as follows. In the next section, we review some related work. In Section 3, based on analysis using the non-zero–sum game theory, we propose to incorporate a constraint mechanism with feedback and evaluation to construct a pro-active access control model for the mobile networks. In Section 4, we perform some simulation to show how the behavior of subjects in mobile networks can be constrained through the constraint mechanism in the access control model based on non-zero-sum game theory. Finally, in Section 5, we conclude this paper in which we also discuss our future work.

2. Related Work

The concept of access control is introduced by Lampson in 1971 in which access control matrix model was proposed [3]. In the model, the rows of the matrix represent subjects who make access requests actively, and the columns represent objects who respond to these access requests passively. And each matrix entry records an access permission that the corresponding subject has to the corresponding object. Since then, access control has been developed into many models because of their different access control policies. Among these models, there are three mainly types: discretionary access control (DAC) [4], mandatory access control (MAC) [5] and role-based access control (RBAC) [6-7]. The three types of access control model serve different mechanisms of access control policies. But all these models are identity-based because they are based on the identification (and authentication) of a subject, either directly or through a mapping from a subject to a role that can be assigned dynamically to a subject. So DAC, MAC and RBAC are effective for closed environments such as an organization that deals with a set of known users who access a set of known services within the organization.

As the development of computer science, the network environment is more and more open, especially the appearance of mobile networks, in which the real identities of subjects is unknown so that there are more and more threats and attacks like intrusion [8], phishing [9], viruses [10], cybercrimes [11]. To solve this problem, experts have done many researches and proposed some access control models such as context-based access control (CBAC) [12] and attribute-based access control (ABAC) [13]. But each model has its advantages and disadvantages, and not solves the security problem completely. So we introduce non-zero-sum game theory to the access control model to solve the security problem in mobile networks.

3. The Access Control Model based on Non-zero-sum Game Theory (NGTAC)

Our goal is to design an access control model which could resist the threats and attacks in mobile networks. To design this model, we use non-zero-sum game theory, so that we call this model NGTAC. In this model, if a subject makes an honest access, he will remain a good impression on the mechanism, and his next access request will be more likely to be permitted by the object; on the opposite, is he makes a dishonest access, he will remain a bad impression on the mechanism, and his next access request will be more likely to be denied by the object. Then, we will introduce the access control model mechanism in detail, especially its non-zero-sum game process between subject and object, which is the most important.

The process of NGTAC includes two participants, six modules and a database. The participants are subject and object. The modules are access evaluation module (AEM), access permission determination module (APDM), non-zero-sum game theory analysis module (NGTAM), decision-making module (DMM), result evaluation module (REM), and access feedback module (AFM). The database is to store the prior information of each subject. The access flowchart of NGTAC is shown is Figure 1.

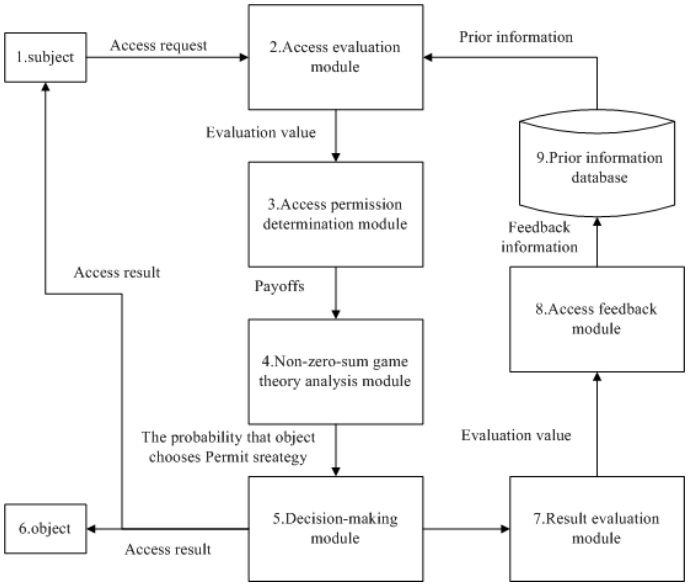


Figure 1. The Access Flowchart of NGTAC

The first step of the process is that subject proposes an access request to the mechanism to ask for some permission. We can see this request as a set of access IP address, access time, access conditions and request permission matrix.

Then in Step 2, the AEM will extract the subject's IP address, access time, access network conditions and get subject's prior information from prior information database. From the four elements above, AEM will compute the evaluation value for the subject and send it to the next module APDM. To define the relation between IP address, access time, network condition and priot information and evaluation value, we suppose that each element has four cases, and divide evaluatoin interval into four disjoint subintervals. Each case of the four elements corresponds to a subinterval. For example, the trust interval is A= [0, 1], the relations between the four factors and trust computation is shown in Table 1.

Table 1. The Relation between the Four Elements and Evaluation Value

IP address	very dangerous	dangerous	safe	very safe
Access time	Never	occasional	normal	frequent
Network condition	very dangerous	dangerous	safe	very safe
Prior information	very dangerous	dangerous	safe	very safe
Evaluation value	[0, 0.25)	[0.25,0.5)	[0.5, 0.75)	[0.75, 1]

Then the evaluation value is the weighted average of these elements. The computation formula is as follows. e_i represents the elements, w_i represents each element's weight.

$$E_i=e_1w_1+e_2w_2+e_3w_3+e_4w_4,\ w_1+w_2+w_3+w_4=1 \tag{1}$$

In Step 3, the APDM gets the evaluation value from AEM and computes the permissions that the subject is allowed to possess based on E_i. And according to these permissions, the APDM compute the payoffs for the two players in NGTAM. We sign the request permission matrix from subject as M_1. Based on E_i, we can use formula (2) to compute the permission matrix that the subject could have on this evaluation value. We sign this matrix as M_2. Then through an entry-by-entry intersection of the corresponding values in M_1 and M_2, we get the permissions matrix M_3 that the subject is allowed to possess.

$$M_2 = F(E_i) \tag{2}$$

Based on the permission matrix M_3, the mechanism could calculate the income and/or loss payoffs for the objects and the subject when they choose different strategies which is shown is Table 2.

Table 2. The Payoffs that Subject and Object Would Get

Objects \ Subjects	Honest access	dishonest access
Permit access	$O_{permit}^{honest}, S_{permit}^{honest}$	$O_{permit}^{dishonest}, S_{permit}^{dishonest}$
Deny access	$O_{permit}^{honest}, 0$	$O_{deny}^{dishonest}, S_{deny}^{dishonest}$

In Step 4, there is a non-zero-sum game between subject and object. In a game, there should be three basic elements: players, strategies and payoffs. Using game theory to analyze access control, the players exist naturally; they are the subject who makes access requests and the object who deal with these requests. And to the player subject, his strategies are to be honest or to be dishonest when he makes requests. To the player object, his strategies are to permit or to deny the subject's requests. From Step 3, we have got the payoffs when subject and object choose different strategies in Table 2. Using the classical line drawing method to analyze the payoffs in Table 2, we get the conclusion that there is no pure Nash equilibrium in this game. So we should seek for the mixed Nash equilibrium with derivation method. Supposing that the revenue matrix of object is M_{object}, and it is composed by the payoffs of the object. Similarly, the revenue matrix of subject is $M_{subject}$.The probability that an object chooses permit strategy is supposed as x. Then the mixed strategy for the object is $P_o=(x, 1-x)$. Similarly, the probability that a subject chooses an honest strategy is supposed as y. And the mixed strategy for the subject is $P_s=(y, 1-y)$. Consequently, the payoffs function of subject $E_{subject}$, which is shown below.

$$\begin{aligned} E_{subject} &= P_o \times M_{subject} \times P_S^T = (x,1-x) \times \begin{bmatrix} S_{permit}^{honest} & S_{permit}^{dishonest} \\ 0 & S_{deny}^{dishonest} \end{bmatrix} \times (y,1-y)^T \\ &= x \times S_{permit}^{honest} \times y + x \times S_{permit}^{dishonest} \times (1-y) + (1-x) \times (S_{deny}^{dishnoest}) \times (1-y) \end{aligned} \tag{3}$$

We compute the derivative of $E_{subject}$ on y, and get formula (4):

$$\frac{\partial E_{subject}}{\partial y} = x \times \left(S_{permit}^{honest} - S_{permit}^{dishonest} + S_{deny}^{dishonest} \right) - S_{deny}^{dishonest} \quad (4)$$

Making the formula above to be 0, we can get the value of *x* in formula (5):

$$x = \frac{S_{deny}^{dishonest}}{S_{permit}^{honest} - S_{permit}^{dishonest} + S_{deny}^{dishonest}} \quad (5)$$

Similarly, we can get the value of *y* in formula (6):

$$y = \frac{O_{deny}^{dishonest} - O^{dishonest} permit}{O_{permit}^{honest} - O_{permit}^{honest} - O_{permit}^{dishonest} + O_{deny}^{dishonest}} \quad (6)$$

Then, the probability that object's choosing permit strategy *x* will be post to DMM to support decision-making.

In Step 5, DMM receives the probability that object's choosing permit strategy. And there is a threshold in the mechanism which will be compared with the probability. If the probability is bigger than the threshold, the mechanism will permit the subject's access request and give all permissions the subject could possess at last; if the probability is smaller than the threshold, the mechanism will deny the subject's access request at last. The threshold is a measurement that makes sure the security of system. So the threshold can be specified rather flexibly according to access control policies. If the system also has some other protective measures like firewalls, intrusion detection, etc., the threshold could be set at a lower level so that the system to serve more access requests. On the other hand, if the system is vulnerable to outside attacks, the threshold should be raised so that the system could provide the necessary security protection.

After the decision-making, the decision will be send to the object to be executed, and the access result will be send to the subject at the same time in step 6. Until now, the access process is finished.

In Step 7, REM will make evaluation on the result to prepare for the feedback module. When we compute the evaluation value *C*, we use the formula as follows:

$$C = F(z) = 1 - a^{z}, 0 < a < 1 \quad (7)$$

In the formula, *a* is a parameter from (0,1). The mechanism can determine the value of *a* according to its need. It is obvious that the bigger the value of *a* is, the smaller the changing trend of *C* is, and the smaller the influence to the feedback information is. So when there are some other protective measures, the value of *a* should be bigger. And on the opposite, when the system is vulnerable to outside attacks, the value of *a* should be smaller. And *z* represents the value of damage or goodness subject brings to objects because its malicious behavior or honest behavior. If the mechanism find that the subject's access results in damage to the system, for example, the permissions that subject requests is more that what he could get, *z* will be a negative number, it proves that subject has chosen malicious strategy this time, *C* will be a negative number from [$-\infty$,0). And *C* will reduce rapidly as the damage brought by subject's malicious behavior reduces. And if the

subject makes access normally, the mechanism will give a positive number to *z*, *C* will be a positive number from [0,1). And *C* will increases slowly as the goodness brought by subject's honest behavior increases.

Then in step 8, the AFM will get the value of *C* and compute feedback information as prior information to the database. If *C* is a positive number, *PI'* next time will be bigger than it is this time, and if *C* is a negative number, *PI'* will be smaller next time than it is this time. The compute formula of *PI'* is as follows, *b* and *d* are factors determined by the mechanism:

$$PI' = \begin{cases} PI \times \left(2 - b^{C}\right), 0 < b < 1, 0 < C \le 1, \left(2 - b^{C}\right) < 1 \\ PI, \left(2 - b^{C}\right) = 1 \\ PI \times d^{C}, d > 1, C < 0 \end{cases} \tag{8}$$

From the flowchart of NGTAV, we can see that the permissions subject could get are dynamically changing with the change of prior information of the subject and the network environment about the subject. And the prior information is determined by the subject's access attitude. If subject makes honest access, he will have better prior information through the process of NGTAC, and his evaluation will be bigger so that he will have more permission to be passed next time. On the opposite, if he makes dishonest access, he will have worse prior information through the process of NGTAC, and his evaluation will be smaller so that he will have less permission to be passed next time. This mechanism drives subject to be more honest in mobile networks.

4. Simulation and Result

To evaluate the effectiveness of our access control model based on non-zero-sum game theory in mobile networks, we have performed some experiments to compare it with traditional access control. In these experiments, we suppose that there are 10 objects and 200 pads or phones as subjects and the subjects are divided into two sets S1 and S2 in average. Subjects in S1 make access requests to the objects under the protection of a traditional access control model and those in S2 make access requests to the objects under the protection of NGTAC. The evaluation metric is the probability that the subjects and the objects choose the cooperative strategy (honest, permit) as their actions. In the scenario, the subjects in S1 and S2 all make accesses with a middle probability 0.5 as the original probability to choose honest strategy. We repeated the scenario 1000 times from which we randomly pick the results of 30 continuous accesses from some stages. And we repeated this experiment 100 times and compute the average value. The result of the scenario is shown in Figure 2.

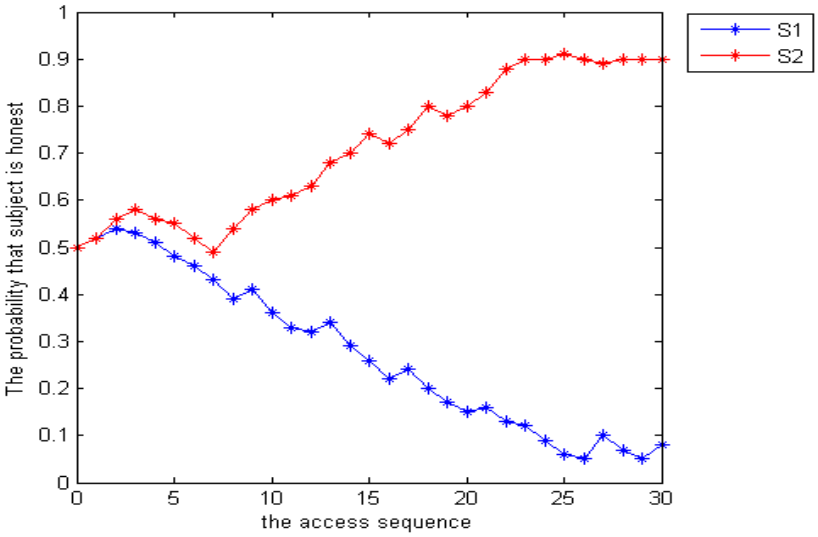


Figure 2. The Probabilities that Subject's being Honest in Different Situations

From Figure 2, we see that in the traditional access control model, the average probability that the subjects in S_1 choose honest strategy is downloading until it fluctuates around 10%. It means that subjects tend to betray the cooperation because they don't need to worry about the punishments from the access control model in this situation. So when they make actions, what they need to consider is only that which strategy would bring them more payoffs. But in the NGTAC, the average probability that subjects in S_2 choose honest strategy is uploading until it fluctuates around 90%. It means that subject tends to maintain the cooperation because there are punishments to their dishonest behavior in this situation. If they are dishonest this time, the permissions that they could get next time will be reduced. So when they make actions, what they need to consider is that which strategy would bring them more payoffs now and in future, so subjects in S_2 tend to be more honest.

From the analysis above, it is obvious that in the NGTAC, we reduce the subjects' dishonest behavior and make them more honest. Then the objects will face less threats and risks.

5. Conclusion

In this paper, we proposed an access control model based on non-zero-sum game theory NGTAC to response to the threats and attacks in mobile networks. In NGTAC, we design the process into some modules and introduce each function of the modules in detail. Then we make some experiments to compare the probabilities that subjects being honest in NGTAC with those in traditional access control models to see the effectiveness of NGTAC. In the future, we will do more work on how to make this model to adapt to a large amount of disorder access requests from subjects.

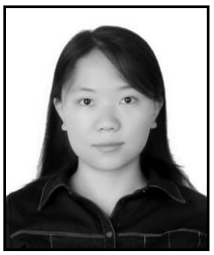
Acknowledgements

The work in this research has been supported by National Natural Science Foundation of China (61272500), Beijing Natural Science Foundation (4142008), the Pre-launch of Beijing City Government Major Tasks and District Government Emergency Projects (Z131100005613030) and Shandong National Science Foundation (ZR2013FQ024).

References

[1] S. Phelps, M. Marcinkiewicz and S. Parsons, "A novel method for automatic strategy acquisition in N-player non-zero-sum games", Proceeding AAMAS '06 Proceedings of the fifth international joint conference on Autonomous agents and multivalent systems, New York, USA, (**2006**), pp. 705-712.
[2] C. Daskalakis, P. W. Goldberg and C. H. Papadimitriou, "The Complexity of Computing a Nash Equilibrium", SIAM Journal on Computing, vol. 39, no. 1, (**2009**), pp. 195–259.
[3] B. W. Lampson, "Protection", Proceedings of the 5th Princeton Symposium on Information Sciences and Systems, (**1971**), pp. 437-443.
[4] S. Lawrence, "Formal Models of Capability-Based Protection Systems", IEEE Transactions on Computers, vol. C-30, no. 3, (**1981**) March, pp. 172-181.
[5] D. E. Bell and L. LaPadula, "Secure Computer Systems: A Mathematical Model", Mitre Corporation, Bedford, MA, (**1973**).
[6] S. Ravi S, C. Edward J, F. Hal L and Y. Charles E, "Role-based Access Control Models", Computer, vol. 29, no. 2, (**1996**) February, pp. 38-47.
[7] D. Ferraiolo and D. Kuhn, "Role-based Access Control", Proceedings of the NIST-NSA National Computer Security Conference, (**1992**), pp. 554-563.
[8] W. A. Wulf and A.K. Jones, "Reflections on Cybersecurity", JScience, vol. 326, (2009), pp. 943-944.
[9] F. R. Chang, "Is Your Computer Secure?", J.Science, vol. 325, (**2009**), pp. 550-551.
[10] K. Gammon, "Four Ways to Reinvent the Internet", Nature, vol. 463, (**2010**), pp. 602-604.
[11] A. Martin. "How Safe Are Your Data?", Nature, vol. 464, (**2010**), pp. 1260-1261.
[12] H. Yao, H. Hu, Z. Lu and R. Li, "Dynamic role and context-based access control for grid applications", IEEE Region 10 Annual International Conference, Proceedings/TENCON, vol. 2007, (**2007**).
[13] B. Wang and L. Wang, "Design of attribute-based access control model for power information systems", Dianli Xitong Zidonghua/Automation of Electric Power Systems, vol. 31, no. 7, (**2007**), April 10, pp. 81-84+98.

Authors



Yi-xuan Zhang, she is a Ph.D. candidate in the School of Software Engineering at Beijing University of Technology, Beijing, China. She received her B.S. degree in Beijing University of Technology in 2011. Her research interests include network security, access control, game theory and distributed network technology.

Jing-sha He, he is a professor in the School of Software Engineering at Beijing University of Technology (BJUT) in Beijing, China. He received a Ph.D. degree from the University of Maryland at College Park in 1990. Prior to joining BJUT in 2003, he worked for IBM, MCI Communications and Fujitsu Laboratories engaging in R&D of advanced networking and computer security. Prof. His main research interests include information security, network measurement, and wireless ad hoc, mesh and sensor network security. He has published nearly 200 papers in the above areas.

Ruo-hong Liu, he is the General Manager of the IT Department at Beijing Development Area Co., Ltd in Beijing, China. His interests include enterprise cloud computing and information security.

