Journal of Computing and Electronic Information Management

ISSN: 2413-1660

An Access Control Strategy Based on ARBAC97 Model for SDN Controller

Hui Huang[1, a], Chuan Liu[1, b], Qian Niu[2, c], Wenjing Zeng[2, d]

[1]Institute of information and communication, Smart Grid Research Institute of National Grid, Beijing, China

[2]School of control and Computer science engineering, North China Electric Power University, Beijing, China

[a]huanghui@sgri.sgcc.com.cn, [b]liuchuan@sgri.sgcc.com.cn, [c]nijiushihao@163.com, [d]zwj_urumqi@163.com

Abstract: With the advantages of distributed architecture, and centralized network control, SDN (Software Defined Network) is much more extensible and has a broad application prospects. However, SDN is faced with many security threats at the same time, such as threats in controller security and the South / North Channel security. Addressing the problems of illegal access to the controller, this paper proposes an improved RBAC access control model which is based on ARBAC97 model and can be applied in SDN. This model improves the existing trust calculation method by using a dynamic authorization strategy and taking the time characteristic factor into consideration. Problems of dynamic allocation of rights in the large-scale complex application can be successfully solved by calculating multiple trust features of users. At the end of this paper, the process of its dynamic authorization is discussed.

Keywords: SDN, Access control, trust calculation, authorization strategy

1. Introduction

Software-defined networking (SDN) is a new network architecture which meet the needs of the future Internet. It separates the network control plane from the underlying network and uses software mode of control plane to replace the traditional closed control plane. SDN uses a centralized controller to manage the entire network and allows network programming [1]. SDN has brought great changes to the network because of its openness and flexibility, but also faces many security threats, especially the security threat of the controller. If the controller is paralyzed, the entire network will

be paralyzed. If the controller is malicious controlled, the whole network will become a zombie network.

Reference to the method that used to solute the attacker illegal connect to the traditional Web server, we use the RBAC(Role-Based Access Control) strategy to set specific access rights to the SDN users, specify which users can access the controller and how to access, and carry out strict authentication to prevent unauthorized access. The traditional RBAC simplifies the process of system authorization management. It isolated the user principals and the access rights to the object by introducing concept of role and realized the principle of privilege minimization. However, traditional RBAC still exist some problems. First, authority division is only limited to roles. In general multi-user application system, users collaborate to accomplish specific tasks, so work task is the smallest unit of authority division. In the traditional RBAC model, when users who have multi positions use the system, the system will assign roles based on the different positions, so users need to switch between multiple roles. Liu Qiang, the Key Laboratory of CIMS, Guangdong University of Technology, analysised of the existing problems from the core theory role of RBAC[2]. Zhu Jun, ZhongShan University, proposed a access control model based on role and task [3]. Zhao Jing proposed a method of assigning user rights based on data objects [4], she try to manage the rights depends on different data objects that are acquired by users or different task states. Second, RBAC have shortcomings in dynamic customization. The traditional RBAC is essentially established on the static subject-object view, but in multi user cooperative system, the information processing mechanism is distributed and hierarchical, so we need Dynamic authorization mechanism. Li Qin, in AnHui University of science and technology, put forward that use dynamic authority list to solve traditional RBAC problems in dynamic allocation of authority. SuWei designed a dynamic RBAC model considering the credibility of the user. This model introduces the concept of role instances and user credibility [7], so that the authorization can be realized through different role instances. It makes authorization mechanism more flexible, but the time characteristic problem is not considered in it. To some extent, these methods can alleviate the shortage of traditional RBAC.

On the basis of analyzing the advantages and disadvantages of the existing research work, this paper proposed a dynamic RBAC model based on multi-dimensional trust (MDT-RBAC), which is an extension of role management model ARBAC97. The model introduces time characteristic factors to improve the existing calculation method of trust. Besides, it synthetically computes a variety of trust characteristics of users, so as to fulfil flexible and dynamic authorization mechanism.

2. Multi-dimensional trust algorithm

In this paper, we use the standard of general evaluation for human in the interpersonal society, comprehensive considered the four indicators: Feedback Trust between nodes, Evaluate Trust between nodes, node's Prestige Trust in system and Criminal Record Trust. The calculation rules of each index are as follows.

2.1 Feedback Trust (FTrust)

Feedback refers to evaluation of access node to the visited node in distributed system, it can expressed as follows [6].

$$\mathrm{FTrust}_{ijm} = \frac{\sum_{k=1}^{m} Sat_{ij}}{m} \times \frac{m}{n} \beta^{\frac{1}{m}} \tag{1}$$

m means the total number that node i visit node j, n means the total number that node i visit all the nodes, FTrust_{ijm} is Feedback Trust of node i visit node j m times, Sat_{ij} is the access evaluation function for node i visit node j once, $Sat_{ij} \in [0,1]$, β is Trade density adjustment constant, $\beta \in (0,1)$.

Based on formula (1), this paper considers the time characteristic. It means previous access cases play a much smaller role over time. So we improve the calculation of the Feedback Trust as follows:

$$FTrust_{ijm_{tp}}^{tp} = \frac{\sum_{k=1}^{m_{tp}} Sat_{ij}}{m_{tp}} \times \frac{m_{tp}}{n_{tp}} \beta^{\frac{1}{m}} \times f(tp,t) \tag{2}$$

$FTrust_{ijm_{tp}}^{tp}$ means the Feedback Trust that node i to node j in fixed time slice tp, other parameters which are the same with formula (1) are all based on time slice tp, $f(tp,t)$ means the trust effectiveness of time t relative to time slice tp, it's a decreasing function, as follows:

$$\mathrm{f(tp,t)} = 1 - \alpha\left(\frac{t-tp}{t}\right) \tag{3}$$

α is attenuation coefficient, $0 \leq \mathrm{f(tp,t)} \leq 1$.

Finally, we get the node i to node j's Feedback Trust when the time arrive t:

$$\mathrm{FTrust}_{ij} = \sum_{t_0}^{t} FTrust_{ij}^{t} \tag{4}$$

t_0 means time slice of the first time that node i visit node j.

2.2 Evaluate Trust (ETrust)

The evaluation similarity refers to the similarity of satisfactory degree between the interactive nodes in the system.

$$\mathrm{ESat}_{ijm} = \sum_{k=1}^{m} \frac{Sat_{ij}}{m} \tag{5}$$

This paper references the method of removing the highest and the lowest values in sports competitions. There is an agreement that if Sat_{ij} is larger than the maximum threshold value or smaller than the minimum threshold value, the Sat_{ij} will be removed. Assume that there is a node which meets the condition above, the trust similarity generated from the time when the node i is accessing the node j is:

$$\mathrm{ETrust}_{ij} = 1 - \sum_{k=1}^{i} \frac{(Sat_{ik} - \mathrm{ESat}_{ij})^2}{i} \tag{6}$$

2.3 Prestige Trust (PTrust)

Prestige indicates the accepted credibility of a node in the whole scope, which would not change with the view of similarity between different nodes and other nodes. Its value is set when the node enters the system, and this value would be valid and not changed until the node gains prestige promotion in some way.

PTrusti that means the prestige trust of Node i in the system could be set into three kinds, Low Mid and High. The initial prestige of the ordinary node is set to Low, and that of the administrator node is set to High. Only when the prestige is higher than or equal to the minimum value that is set, the node could be visited.

2.4 Criminal Record Trust (CTrust)

Criminal is the major accidents in the running process of the node. For example, when Node i accesses Node j, if Node i conducts a serious cheat, it is considered that Node i is not reliable, and the action is marked as a criminal. The criminal of Node i, CTrusti, is divided into three tags, No Cheat, Normal Cheat and Serious Cheat according to the degree to cheat other nodes, those are expressed as NoC, NorC and SC separately. The target node would be to do the criminal evaluation according to the degree of tolerance for the cheat. The mean of criminal evaluation is only to exclude the nodes that couldn't be accessed and not to select the accessed nodes. According to the above 4 indicators, the multi-dimensional trust that node i visit node j can expressed as follows:

$$Trust_{ij} =< FTrust_{ij}, BTrust_{ij}, FTrust_{i}, CTrust_{i} > (7)$$

3. MDT-RBAC model

3.1 MDT-RBAC model structure

Extend the traditional role management model ARBAC97 and synthesize multi-dimensional trust of users, this paper achieve a dynamic and flexible authorization mechanism, so that make the process that system allocates the required permissions for users more secure and flexible. Basic elements of the MDT-RBAC model include Users, Groups, Roles, Sessions, Permissions and Trust. Users get object access permissions indirectly through roles. It's a many-to-many relationship between users and roles, roles and permissions. It means a user can have multiple roles, a role can also be assigned to multiple users. As the same, A role can be granted to multiple permissions, a permission can also be granted to multiple roles. During the process of authorization, we need to match the trust information. Only when the trust degree is satisfied, users can obtain the appropriate access rights. Figure 1 is the MDT-RBAC model structure.

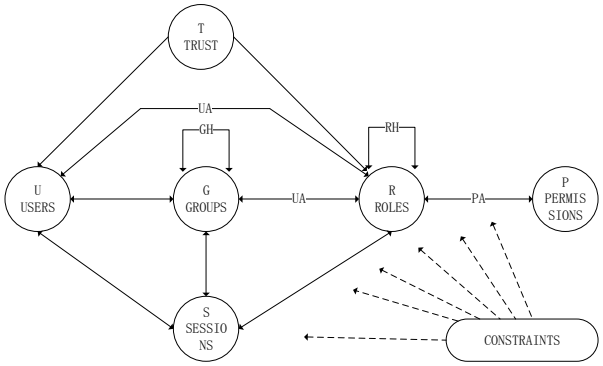

Figure 1. Model structure MDT-RBAC.

3.2 Component elements of the MDT-RBAC model

The improved model is represented as a six tuple<U, G, R, S, P, T>, for the Users, Groups, Sessions, Roles, Trust 和 Permissions, respectively. Every elements and their relationships are described as follows:

U: Users ={$user_1$,$user_2$,..., $user_n$ }, Users can be expressed as a specific user, it can also be expressed as the system of active entities.

G: Groups = Users{Users1 ,Users2,...,$Users_n$ }, is a group of users with the same role.

R: Roles = role{role1 , role2,...,rolen }，means right that active entities in the system to access and operate.

S: Session set, Users establish a session to access resources, each Session establishes a mapping relationship between the user and corresponding role set.

P: Permission set, Permissions = p{ p1 , p2,...,pn}, represents the permission of accessing the system unit, P_i = (op,s, LimTrust), s means object, LimTrust indicates threshold value of the trust when the authority is granted.

T: trust，it' s according to the trust algorithm and it' s a constraint relationship between users and roles.

$UA((U \times R) \cup (G \times R))$：Express correspondence between users and roles. Users can directly obtained the required roles or from the user group.

$GH(G \times G)$：Represents a hierarchical relationship between Users. The lower user group is a subset of the roles that the upper user group have.

$RH(R \times R)$：Represents a hierarchical relationship between Roles. The lower roles' authority is a subset of the upper roles' authority.

$PA \subseteq (P \times R)$：Indicates the distribution relationship between roles and authorityies, it's a Many-to-many relationship.

$UTR((U \times T) \cup (G \times T))$：Represents a trust value that user or user group assign roles. The relationship between user or user group and trust value is Many-to-many, it means a user has different trust values for different applications.

4. MDT-RBAC in SDN

4.1 The whole structure

The function frame structure of Improved RBAC model in the SDN as shown below, it includes group management, user management, role management, trust management, permission management and authorization management. In that, group management also includes autonomous group and administrator management of autonomous group. Permission management include functional authority management and data authority management. Authorization management include user-role authorization, role-permission authorization and group- permission authorization.

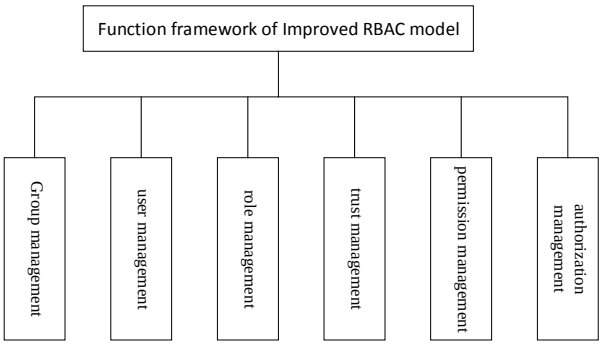

Figure 2. The function frame structure of Improved RBAC model

Group management, user management, role management are the maintenance of basic data. Permission management establish functional authority and data authority according to existed users. Authorization management means autonomous group administrator can distribute the corresponding functional authority and data authority for roles based on the actual needs of the application, then give the role to the user or give the functional authority and data authority to sub autonomous group. Thus, an authorization process was completed. This process include UA and PA process for users in extended RBAC model.

4.2 Dynamic authorization process

The improved authorization is different from the traditional RBAC authorization method. First, after the user through the identity authentication login to SDN controller, improved RBAC model will distribute some non-activation basic role for user based on his identity, this role can be understood as a collection of roles that the user may get the most permissions. Then, users access to a specific node according to their own needs. Now, according to the value of the Trustij whether meet the requirement, MDT-RBAC will activate the corresponding role. Trustij requirement is one of the access threshold (LimTrust) which is set by the target node. Target node can set different threshold and threshold requirements for the 3 components of Trustij. For example, target node can set only meet the FTrustij as the threshold value or meet any other combination of 3 components. The threshold value of each component is set by the target node through a certain method, it depends on the specific needs of the target node, the process is shown in the following diagram

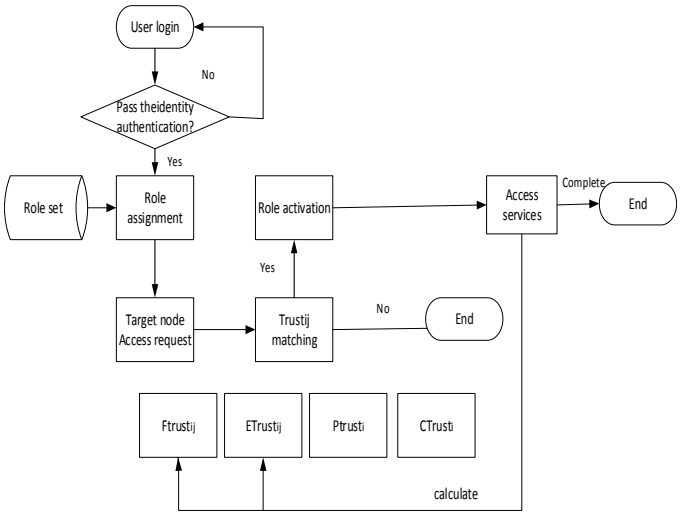

Figure 3. Dynamic authorization process

Specific implementation process is as follows:

Step1 A user logins the system and authenticates his identity. If the user's identity is confirmed, the phase of role assignment comes. Otherwise, return to the page of login.

Step2 According to the user's type, the system will grant the user the highest role. The system will do matching according to the requirements of the target node based on the $Trust_{ij}$ when the user is accessing the target node. If it can be successfully matched, the corresponding role to the target node will be activated. Otherwise, the visit is over and results are returned.

Step3 After activating the role and obtaining the appropriate authority, we should calculate the FTrustij and ETrustij, judging whether they are meet the requirement during the access process. If they are not up to standard, system will revoke the authorities which correspond to the role and set the role to an inactive state, user access to the end. If always up to the standard, user can continue visit the node until the end

Step4 Access process end, set the Trustij that access node to visited node according to the feedback from the target node.

5. Conclusion

This paper discusses the improvement of RBAC model and its application in SDN, The model introduces time characteristic factors to improve the existing calculation method of trust. Besides, it synthetically computes a variety of trust characteristics of users, so as to fulfil flexible and dynamic authorization mechanism. Then, use improved model in SDN controller security protection, we discussed it functional structure and fine-grained dynamic authorization process in SDN. Subsequent research work needs to apply this

model to the actual SDN operating environment. In this paper, we only consider the illegal access problems for SDN controllers, we also need to study the other security threats for SDN network.

Acknowledgments

This paper is funded by the project of The State Grid Corporation of China in 2014 “Research on the software defined network system and its key technology applied in electric power”.

References

[1] DaiBin, WangYuanhang, Yangjun. SDN Security discussion: Opportunities and threats [J]. Computer application research, 2014, 08:2254-2262.

[2] LiuQiang, WangLei, Helin. A series of problems in the research of RBAC model [J]. Computer science, 2012, 39(11):13-18.

[3] Tangyong, ZhuJun. Study of the Access control technology in CSCW system based on role and task. [J]. Computer science, 2010, 37(7): 130-133.

[4] ZhaoJing, YangRui, JiangLuanSheng. RBAC access control model based on data object [J]. Computer engineering and design, 2010, 31(15) : 3353-3356.

[5] Sandhu R., Bhamidipati V, Munawer Q. The ARBAC97 Model for Role-Based Administration of Roles [J]. ACM Trans on Information and System Security, 1999, 2(1):105-135.

[6] LiuWu, DuanHaixin, ZhangHong. TRBAC: Trust based access control Model [J]. Computer research and development, 2011, 48(8): 1414-1420.

[7] SuWei, ZengGuangzhou. A dynamic RBAC model considering the Trust of user[J]. Computer Engineering, 2005, 31(15): 84-86.

[8] Ferraiolo D F, Cugini J A, Kuhn D R. Role-based accesscontrol (RBAC) : Features and motivations [C]/ / Proceedings of the 11th Annual Computer Security Application Conference,1995: 241-248.

[9] SANDHU R S, COYNE E J, FEINSTEIN H L, et al. Role-based access control models [J].IEEE Computer, 1996, 29(2): 38-47.