MD-UCON: A Multi-Domain Access Control Model for SDN Northbound Interfaces

Rui CHANG\textsuperscript{1,a,*}, Zhaowen LIN\textsuperscript{2,b}, Yi SUN\textsuperscript{3,c,*}, Jie XU\textsuperscript{4,d}

\textsuperscript{1}Network and Information Center, Institute of Network Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China Science and Technology on Information Transmission and Dissemination in Communication Networks Laboratory National Engineering Laboratory for Mobile Network Security (No. [2013] 2685) Network and Information Center, Institute of Network Technology / Institute of Sensing Technology and Business, Beijing University of Posts and Telecommunications. Beijing, 100876, China

\textsuperscript{2}Network and Information Center, Institute of Network Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China Science and Technology on Information Transmission and Dissemination in Communication Networks Laboratory National Engineering Laboratory for Mobile Network Security (No. [2013] 2685) Network and Information Center, Institute of Network Technology / Institute of Sensing Technology and Business, Beijing University of Posts and Telecommunications. Beijing, 100876, China

\textsuperscript{3}Network and Information Center, Institute of Network Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China Science and Technology on Information Transmission and Dissemination in Communication Networks Laboratory National Engineering Laboratory for Mobile Network Security (No. [2013] 2685) Network and Information Center, Institute of Network Technology / Institute of Sensing Technology and Business, Beijing University of Posts and Telecommunications. Beijing, 100876, China

\textsuperscript{4}Network and Information Center, Institute of Network Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China Science and Technology on Information Transmission and Dissemination in Communication Networks Laboratory National Engineering Laboratory for Mobile Network Security (No. [2013] 2685) Network and Information Center, Institute of Network Technology / Institute of Sensing Technology and Business, Beijing University of Posts and Telecommunications. Beijing, 100876, China

\textsuperscript{a}changrui@bupt.edu.cn, \textsuperscript{b}linzw@bupt.edu.cn, \textsuperscript{c}sybupt@bupt.edu.cn, \textsuperscript{d}cheer1107@bupt.edu.cn

ABSTRACT In SDN (Software Defined Network) environments, for the security considerations of the upper-layer application behaviors, we need to consider adding an access control mechanism to the northbound interface of the SDN control layer to limit the capabilities of the upper-layer applications, thereby improving the security of the SDN. In addition, considering the performance and management requirements of SDN, access control features including cross-domain support should be considered. In this paper, we proposed an MD-UCON access control...
model with role mechanism extension based on UCON and role-based access control mechanism. At the same time, we introduced a cross-domain role mapping method to support cross-domain access authorization, thereby enabling the model to be applied to the application of access control for the SDN northbound interface.

1. INTRODUCTION

In recent years, with the development of Software Defined Network (SDN), its advantages in terms of openness, reliability, flexibility, control and scalability have become increasingly prominent, and have been received in industry and academia. SDN decouples the control layer from the data layer of networks, allowing users to dynamically configure the network in a programmed manner, thereby simplifying network management and enabling flexible traffic control, also providing a good platform for core network operation and application innovation. However, SDN technology is not yet mature. The SDN northbound interface directly serves the upper layer application, and various control layer systems are implemented based on different technologies, resulting in a decentralized development direction. There is no unified interface standard, and the mainstream SDN software controllers respectively provide completely different northbound interfaces. Most SDN control layer elements provide northbound interfaces, but lack access control mechanisms for upper layers [1][2].

In the absence of the corresponding security mechanism, the security and stability of the SDN are threatened, including, between the application layer and the control layer, there may be application errors, inconsistent application layer and control layer status; when the control layer passes when a northbound interface is connected to multiple applications, problems such as command conflicts and inconsistent application status may occur between multiple applications. When an application error occurs or application is maliciously controlled, it will also bring unpredictable danger to the network [3][4].

Meanwhile, in recent years, with the continuous improvement in all areas of the network demand, it is necessary to fully consider the network scale when deploying SDN networks. When the network reaches a certain scale, the performance of the SDN controller may become a network performance bottleneck [5], also, the large single-domain network is inconvenient in management. Given that multi-domain networking is an effective solution to scale problems, and cross-domain access requirements are becoming more and more urgent, when researching access control mechanisms, further consideration needs to be given to how to build cross-domain access control mechanisms.

Traditional access control models, including Discretionary Access Control (DAC) [6], Mandatory Access Control (MAC) [7], and Role Based Access Control (RBAC) [8][9][10] can meet the requirements and protect resources from unauthorized access under general traditional scenarios. However, the authorizations of these access control models are based on pre-defined rules, and it is difficult to meet the access control requirements of cross-domain access in dynamic and complex scenarios.

In 2002, Park and Sandhu proposed the Usage Control (UCON) model, which integrates the models of access control, digital rights management and trust management, providing fine-grained, continuous access control ability, and meeting the requirements of access control in complex scenarios [11][12][13].

UCON is an abstract model, and its significance is more to provide a scheme to the modeling, rather than directly describe a specific access control mechanism. In order to meet the requirements of multi-domain SDN northbound interface access control better, we extended the UCON model and proposed the MD-UCON model, achieving the SDN northbound interface access control that supports cross-domain access.

The rest of this article is organized as follows. In Section 2, we showed the current researches related to this article. In Section 3, we briefly introduced the UCON model. In Section 4, we described our main contribution, the MD-UCON model. In Section 5, we summarized the work of this paper.
2. RELATED WORKS
The works related to this paper includes researching on the access control of SDN northbound interface in multi-domain SDN environment, proposing the role extended multi-domain access control model, researching cross-domain role conversion mechanism in multi-domain scenarios.

In previous researching, some research efforts attempted to provide access control for SDN northbound interfaces or SDN upper layer applications to improve SDN security. Canini et al. implemented the security verification of third-party SDN applications by means of attribute checking and symbolic execution. However, the proposed verification is not dynamic monitoring at runtime, and the verification is mainly for a single SDN application scenario [14].

Sherwood et al. sliced and partitioned the control logic of different users on the control layer to provide access control based on certain rules for user access, but this processing method can only isolate the control logic between different users [15].

Wen et al. assigned permissions to the commands that can be used by the application layer, which realized the isolation between the application and the control layer kernels, and improved the security and stability of the control layer. The research focuses more on preventing all upper-layer applications from destroying the underlying network. There is no access control for different policies for multiple applications [16].

In particular, Klaedtke et al. proposed an access control scheme for SDN upper-layer applications [17]. The research proposed to use network users as the subjects, and use information and configurations, including statistics, flow rules, as objects. The rights are defined as the set of reading operations and modifying operations. And, the concept of strategy is introduced. The scheme is largely in line with UCON components, such as subject, object, authority, and authorization. This research provides a reference for the work of this paper.

Since previous researches on SDN access control did not adequately consider the need to support scenarios include multiple domains and multiple SDN applications, especially for requirements in multi-domain scenarios, a further research work is still needed.

3. UCON
The Usage Control (UCON) model was first proposed by Park and Sandhu in 2002. UCON integrates the traditional access control, trust management and digital rights management. In terms of access control, UCON covers traditional DAC, MAC and relatively advanced RBAC. The UCON model extends the traditional access control and defines three decisive factors: Authorization (A), Obligation (B) and Condition (C), and brings continuity and mutability to UCON innovatively. This allows UCON to adapt well to highly dynamic, continuously changing scenes.

The UCON model consists of six elements, including subjects, objects, rights, authorizations, obligations, and conditions. The UCON model can be shown by figure [1]. Subjects are entities that contain attributes, holding the rights to subjects. Objects are entities who also contain attributes, who subjects hold rights on. Rights are privileges on accessing objects, holding by subjects. Authorization are a set of rules that should be satisfied before the subject accessing the object. Obligation is the mandatory requirement that the subject must accomplish before accessing the objects. Conditions is a set of decision factors that are verified before subjects accessing the objects.
Compared to traditional access control models, UCON's most outstanding feature is the continuity of decision and mutability of attributes. Continuity of decision means that the control strategy can be executed before and during the access. The control decision component can perform verifications in these two phases, called pre-decision and ongoing-decision. Mutability of attributes means that attributes of subjects and objects can be updated as accessing results. Attribute updates include pre-updates, ingoing-updates, and post-updates. The updating may cause the system to perform actions, including allowing or revoking access rights. Figure [2] shows a completed use process with three phases in time: before-use, ongoing-use and after-use.

In the UCON model, decision factors are composed of authorizations, obligations, and conditions. The UCON model can be classified according to the continuity of decisions and the mutability of attributes. The UCON model can be divided into 24 categories according to the continuity of decision and the variability of attributes. For practical reasons, some models have no practical significance, so there are total of 16 available models. Figure [3] shows all possible models of UCON, where “Y” indicates that the model has practical significance, and “N” indicates that the model has no practical significance. Figure [3] (a) shows the possible combinations of UCONABC models and their relationships. Figures [3] (b), (c) and (d) show possible scenarios in the UCONA, UCONB, and UCONC models, respectively.

Table 1. The 16 Basic ABC Models

|       | 0 (immutable) | 1 (pre-update) | 2 (ongoing-update) | 3 (post-update) |
|-------|---------------|----------------|--------------------|-----------------|
| preA  | Y             | Y              | N                  | Y               |

Figure 1. Structure of UCON Model

Figure 2. Continuity and Mutability of UCON
4. MD-UCON

4.1 Introduction of MD-UCON
In this section, we proposed a Multi-Domain Usage Control (MD-UCON) model by extending the basic UCON model, thereby supporting cross-domain accessing. First, we introduced the domains entities, which are corresponding to the real-world domains, so that the real domains factors can be suitably modeled. Then, we introduced attributes and mechanisms from role-based access control (RBAC), simplifying the complexity of access control mechanism when facing the multi-domain scenarios; Finally, we introduced a cross-domain role mapping mechanism to resolve the problem that the cross-domain access cannot be directly dealt due to the independence of roles from different domains.

4.2 Components of MD-UCON
MD-UCON introduced the concept of domains, which can divide all subjects and objects into finite groups. Therefore, each subject has a property called subjectDomain that represents the domain in which the subject resides; each object also has an attribute named objectDomain that represents the domain in which the object resides. The domains in the model are entities that can hold some attributes, corresponding to real-world domains. For example, in a general SDN deployment, all network elements managed by the same controller, as well as all upper-layer applications directly accessing this controller, belongs to the same domain. According to whether the domain attribute of the subject and object are the same, the access from subject to object can be divided into two categories, intra-domain access and cross-domain access.

MD-UCON also introduced the concept of role, which is a key attribute of the subject and is used for the authentication process of access control. A role is an entity that can contain some attributes. It has a many-to-many relationship with the subject. Each subject has a property called subjectRoles that represents a collection of role attributes held by the subject. When the access occurs, the access control system queries the role attribute set of the access subject. If any of the role attributes meet the permission requirements of the current access, the authentication succeeds. Due to the existing relationship between the role and the subject and the relationship between subject and the domain, the role and the domain also have an indirect many-to-one relationship, that is, a domain may contain a finite number of different
role entities. The introduction of roles entities reduces the complexity of subject attributes and authentication rules, while providing support for cross-domain access control. The extended MD-UCON components and their relationships are shown in Figure [5].

![MD-UCON Model](image)

**Figure 5. MD-UCON Model**

### 4.3 Cross-Domain Role Mapping

The purpose of the cross-domain role mapping mechanism is to solve the problem that role-based access control systems cannot be directly applied to cross-domain access scenarios. The traditional intra-domain role mapping policy can be divided into three categories. The first is the default policy, that is, any external domain role is mapped to a default role in the local domain. In the common case, the default role is the minimum privilege role of the domain. The second is the explicit policy, that is, separated role association, the administrator clearly defines the mapping rules of the external domain role to the local domain role. The third is the implicit policy, that is, after the transfer association mechanism is introduced, a certain implicit policy can be derived from the explicit policy and the role inheritance relationship.

Considering that in the SDN environment, the default policy obviously does not meet the requirements in terms of flexibility; the explicit policy requires the administrator to clearly know all possible roles in different domains and set mapping rules for all possible roles, so the feasibility is unacceptable in practical applications. The implicit strategy with role inheritance may cause the role conflict problem to occur when the rules are set incorrectly. At the same time, the role inheritance mechanism makes the role adding, editing, deleting and other operations have a high complexity in system implementation, and there is also a large system overhead in terms of performance at runtime, therefore using of the strategy should be carefully considered.

In the access control scenario for the SDN northbound interfaces, the authentication rules and the role attributes of the upper application are generally set by trusted administrators. The upper application only holds an immutable access credential, and cannot forge the role and fraud permissions by itself. Under such premises, we can use a new role mapping strategy. We can pre-set a set of public roles in the global scope and raise requirements for each domain: first, any role in any domain must be able to be mapped to a global role; second, each domain is required to has the ability to deal with global roles - either by setting permissions for all global roles, or providing mapping rules for all global roles. By using a global role which can be understood by any domain as an intermediate role, it is guaranteed that any subject can be understood by the access control system when cross-domain access occurs. Since the number of global roles is limited and usually is relatively small, and role rules are easy to set, resulting in a good feasibility of this strategy. Therefore, we solved the problems that the traditional role mapping strategy is not flexible enough and the complexity is too high to be applied.
4.4 Formal Model Definition
The formal definition of MD-UCON is shown as follows:

1) $S$ represents a finite set of subjects. Subjects are entities that initiates access, having role attributes and domain attributes, and may also include general attributes for extension. A user in the SDN network may serve as a subject;
2) $O$ represents a finite set of objects. Objects are the accessed entities, having domain attributes, and may contains general attributes for extension. The statistical information, configuration, flow rules, etc. in the SDN network can be used as objects;
3) $D$ represents a finite set of domains. Domains are entities containing attributes, generally corresponding to the domains in the real world;
4) $\text{ROLE}$ represents a finite set of roles. Roles can contain general attributes for extension;
5) $R$, $A$, and $C$ respectively represent a limited set of permissions, authorization rules, obligations, and conditions, which are the same as the UCON model;
6) $\text{subjectDomain}: (s: S) \rightarrow D$, a function mapping from the subject $s$ to its domain;
7) $\text{objectDomain}: (o: O) \rightarrow D$, a function map from the object $o$ to its domain;
8) $\text{subjectRoles}: (s: S) \rightarrow 2^{\text{ROLE}}$, a function map from the subject $s$ to the set of role attributes it holds;
9) $\text{globalRole}: (\text{role}: \text{ROLE}) \rightarrow \text{ROLE}$, a function mapping from a domain role to a global role, the specific rules are usually set by the administrator;
10) $\text{roleAllowed}: (\text{role}: \text{ROLE}, o: O, r: R)$, is a Boolean function, indicating whether the role has permission to operate $r$ on the object $o$, the specific rules are usually set by the administrators;
11) $\text{innerDomainAllowed}: (s: S, o: O, r: R)$, is a Boolean function, indicating whether the subject $s$ has the permission to operate $r$ on the object of the same domain in a non-cross-domain scenario, which can be represented as:

$$\text{innerDomainAllowed}(s, o, r) = \exists \text{role} \in \text{subjectRoles}(s) \land \text{roleAllowed}(\text{role}, o, r)$$

12) $\text{crossDomainAllowed}: (s: S, o: O, r: R)$, is a Boolean function, indicating whether the subject $s$ has permission to operate $r$ on the object $o$ in a cross-domain scenario, which can be represented as:

$$\text{crossDomainAllowed}(s, o, r) = \exists \text{role} \in \text{subjectRoles}(s) \land \text{roleAllowed}(\text{globalRole}(\text{role}), o, r)$$

13) $\text{allowed}: (s: S, o: O, r: R)$, is a Boolean function, indicating whether the subject $s$ in general sense has the right to operate $r$ on the object $o$, combine the two scenarios of non-cross-domain access and cross-domain access, it can be represented as:

$$\text{allowed}(s, o, r) = \text{innerDomainAllowed}(s, o, r) \lor \text{crossDomainAllowed}(s, o, r)$$

5. CONCLUSIONS
In this paper, the MD-UCON model is proposed by extending the UCON model, to support the access control for the SDN northbound interface, and support the cross-domain access control in multi-domain scenarios. The model introduces the domain entity to enable the modeling of the domain in the real world. By introducing the role entities and the corresponding mechanisms, the complexity of the subject attribute is reduced, and the settings of access control rules are enabled. Finally, the cross-domain role mapping mechanism is introduced, achieving access control in a cross-domain access scenario. Compared with the traditional access control model, MD-UCON meets the requirements of SDN northbound interface access control, with higher flexibility and finer granularity of control, while ensuring a lower complexity, therefore it’s more suitable for SDN northbound interface access control with multi-domain requirements.

ACKNOWLEDGEMENT
This work is supported by the National Natural Science Foundation of China (Grant no. 61601064), the Fundamental Research Funds for the Central Universities (2018RC55), and the Beijing Talents
Foundation (Grant. no. 201700020124G062), the Fundamental Research Funds for the Central Universities.

REFERENCES

[1] Pang Tao, Wei Huanyu, Wu Juan, Chen Jian. Research on the Development Status and Trends of SDN Northbound interface. China Internet, 2014(9).

[2] SHI Zhikao, ZHU Guosheng. Research on security of software-defined networking. Journal of Computer Applications, 2017, 37(S1):75-79.

[3] Scott-Hayward, S., Natarajan, S., & Sezer, S. (2016). A Survey of Security in Software Defined Networks. IEEE Communications Surveys and Tutorials, 18(1), 623-654. DOI: 10.1109/COMST.2015.2453114

[4] ZUO Q Y, ZHANG H S. Analysis and Research on Network Security for OpenFlow-based SDN[J]. Netinfo Security, 2015, (2):26-32.

[5] Kandula S, Sengupta S, Greenberg A, et al. The nature if data center traffic: measurements & analysis[C]/Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference. ACM, 2009:202-208

[6] Thuraisingham B. Mandatory Access Control[J]. NFS vulnerabilities, International Symposium on Collaborative Technologies and Systems, 2013, 29(9):114-116.

[7] Moffett J, Sloman M, Twidle K. Specifying Discretionary Access Control Policy For Distributed Systems[J]. Computer Communications, 1990, 13(9):571-580.

[8] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-Based Access Control Models[J]. Computer, 1996, 29(2):38-47.

[9] Sandhu R, Ferraioolo D, Kuhn R. The NIST model for role-based access control: towards a unified standard[C]/ ACM Workshop on Role-Based Access Control. ACM, 2000:47-63.

[10] US Department of Commerce, NIST. Role Based Access-Control (RBAC): Features and Motivations[J]. December, 1995.

[11] Park J, Sandhu R. Towards usage control models: beyond traditional access control[RAC]:// ACM Symposium on Access Control MODELS and Technologies. DVLBP, 2002:57-64.

[12] Park J, Sandhu R. The UCON ABC usage control model[J]. Acm Transactions on Information & System Security, 2004, 7(1):128-174.

[13] Sandhu R, Park J. Usage Control: A Vision for Next Generation Access Control[J]. Lecture Notes in Computer Science, 2003, 2776:17-31.

[14] Canini M, Venzano D, Peresini P, et al. A NICE way to test OpenFlow applications[C]/Proc. of the 9th USENIX Symp. on Networked Systems Design and Implementation (NSDI), 2012:10.

[15] Sherwood R, Gibb G, Yap K, et al. Can the production network be the testbed?[C]/Proc. of the 9th USENIX Conf. on Operating Systems Design and Implementation (OSDI), 2010:1-6.

[16] Wen X, Chen Y, Hu C. Towards a Secure Controller Platform for OpenFlow Applications[C]/HotSDN, 2013:171-172.

[17] Klaedtke F, Karame GO, Bifulco R, Cui H. Access control for SDN controllers. In: Proc. of the 3rd Workshop on Hot Topics in Software Defined Networking. Chicago: ACM, 2014. 219-220. [doi: 10.1145/2620728.2620773]