Software-Defined Space-Ground Integrated Network Access Authentication Architecture and Methods: Postprint

Authors: Hu Zhiyan, Du Xuehui, Cao Lifeng

Date: 2018-05-18T00:00:00+00:00

Abstract

Space-ground integrated networks exhibit characteristics such as network heterogeneity and dynamics, intermittent connectivity, and highly exposed nodes due to their complex structure. To ensure security, it is necessary to investigate proprietary access authentication architectures and methods. First, by leveraging the Software-Defined Networking principle of separation between control plane and data plane and integrating it with space-ground integrated information networks, a novel access authentication architecture is proposed. The authentication architecture and process are described in detail, enabling security protection for the network and optimized resource control. Subsequently, based on the architectural characteristics, seven attributes influencing access point decision-making are identified, and calculation formulas for each attribute are presented. By combining the Analytic Hierarchy Process with the Technique for Order Preference by Similarity to Ideal Solution, an access point decision-making algorithm is proposed. Experimental simulation results demonstrate that the access point decisions are accurate and enable rational resource utilization.

Full Text

Preamble

Title: One Access Authentication Architecture and Method for Software-Defined Space-Ground Integration Network

Authors: Hu Zhiyan[1],[2], Du Xuehui[1],[2], Cao Lifeng[1],[2]
[1] Information Engineering University, Zhengzhou 450001, China
[2] State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China

Abstract: Due to its complex structure, the space-ground integration network exhibits characteristics such as heterogeneous dynamics, intermittent connectivity, and highly exposed nodes. To ensure security, specialized access authentication architectures and methods must be investigated. First, leveraging the software-defined networking (SDN) principle of separating control and data planes, this paper proposes a novel access authentication architecture that integrates SDN with space-ground integration information networks. The authentication architecture and process are described in detail, enabling both network security protection and optimized resource control. Then, according to the architectural characteristics, seven attributes influencing access point decisions are proposed, along with their calculation formulas. Combining the analytic hierarchy process (AHP) with the technique for order preference by similarity to an ideal solution (TOPSIS), an access point decision algorithm is proposed. Experimental simulation results demonstrate that the algorithm makes accurate access point decisions and achieves rational resource utilization.

Keywords: space-ground integration network; software-defined network; access authentication architecture; decision attribute; decision algorithm

0 Introduction

With the continuous development of satellite networks and expanding cyberspace demands, various strategic information missions have extended from single-dimensional land and sea operations to multi-dimensional sea, air, and space operations. Traditional networks struggle to meet these increasingly diverse requirements, necessitating the integration of ground and space-based networks to form a space-ground integration information network capable of providing diversified services. However, due to its complex structure, the space-ground integration information network exhibits characteristics of network heterogeneity, dynamic behavior, intermittent connectivity, and highly exposed nodes [1]. Research on security technologies is required to ensure normal network operation, and access authentication represents an effective means of guaranteeing security. Therefore, constructing an efficient and flexible access authentication architecture for space-ground integration information networks is essential for providing secure services.

Since the concept of software-defined networking (SDN) was proposed, its applications have rapidly expanded to telecommunications operator networks, data centers, and Internet company business deployments. However, research on SDN-based space-ground integration information networks remains in its infancy. Wang [2] proposed a software-defined satellite network architecture employing a hierarchical structure with a centralized controller at each layer, all controlled by a control center. Chen et al. [3] proposed an SDN-aggregated space-ground integration information network architecture dividing the network into space, air, and ground layers, where the space layer communicates tradi-

tionally while the air and ground layers deploy SDN controllers to coordinate resource allocation and achieve optimized flexible management. Iqbal et al. [4] presented an SDN-based space network architecture that leverages knowledge of aerial node orbits to predict future network events, particularly link disruptions, and proactively mitigates their impact through SDN-based optimization. Li et al. [5] proposed deploying SDN-based multifunctional payload platforms at critical space network nodes and combining SDN architecture with space delay-tolerant network protocols to build a space-based information network, using resource virtualization to achieve on-demand customization and efficient sharing. Existing research on SDN-based space-ground integration information networks remains largely theoretical, with significant implementation challenges, limited simulation realization, and scarce investigation into access authentication for SDN-integrated space-ground networks. There is an urgent need to research easily deployable, optimally managed, secure, and efficient SDN-based space-ground integration network access authentication methods.

1.1 Space-Ground Integration Information Network

The space-ground integration network [6] adopts a dual-plane structure of space and ground, relying on ground networks while extending into space. It interconnects space backbone networks, space access networks, and ground node networks, integrating them with the ground Internet and mobile communication networks. As shown in [Figure 1: see original paper], the space backbone network consists of backbone nodes deployed in geosynchronous orbit, primarily including satellites performing various missions. The space access network comprises nodes deployed in high or low Earth orbit, while the ground node network consists of multiple interconnected ground backbone nodes, mainly including naval vessels and vehicles.

1.2 Software-Defined Networking

SDN originated from Stanford University' s Clean Slate project [7] and was formally introduced by McKeown [8] at the INFOCOM conference in 2009. The SDN architecture [9], illustrated in [Figure 2: see original paper], innovatively employs a layered approach to separate the control plane from the data plane. The data plane handles only data forwarding, while controllers in the control plane use programmable software platforms to centrally control underlying hardware devices, thereby obtaining a global network view and optimizing network control to achieve flexible management and on-demand resource allocation. The control and data planes communicate through open interfaces (e.g., OpenFlow) to issue flow table rules, allowing control applications to focus on their own logic without concerning themselves with underlying implementation details. SDN has been applied across numerous industries and domains, including wireless

networks [10][11][12], network function virtualization [11][13], and data centers and cloud computing [14].

2 SDN-Based Space-Ground Integration Information Network Access Authentication Architecture

2.1 Design Objectives

The space-ground integration information network architecture designed in this paper should achieve the following objectives:

a) **Flexible and Controllable Network:** Traditional space information networks exhibit "stovepipe"development where network element functions are tightly coupled with hardware, making flexible control difficult. The SDN-based space-ground integration information network proposed herein separates control from data, enabling controllers to manage infrastructure based on a global view and achieve flexible controllability.

b) **Converged and Evolvable Network:** Space-ground integration networks comprise multiple heterogeneous networks across ground and space domains, making interoperability challenging. In the proposed SDN-based integrated network, controllers can obtain real-time network status information and schedule resources rationally to achieve convergence among heterogeneous networks.

c) **Customizable Network Services:** Traditional networks struggle to provide on-demand services for users. The SDN-based access authentication proposed in this paper can flexibly provide different authentication services—such as anonymous and concurrent authentication—according to diverse user requirements, enabling customizable services through tailored policies.

2.2 SDN-Based Space-Ground Integration Information Network Access Authentication Architecture

Drawing on the SDN principle of separating control and data planes, we simplify or completely 剥离 control functions from the network infrastructure layer and design a unified security access authentication architecture for space-ground integration information networks, as shown in [Figure 3: see original paper]. The architecture comprises three layers: authentication, control, and device layers.

The **authentication layer** primarily includes a unified access authentication management center responsible for overall access authentication management across the entire space-ground integration information network. It consists of three modules: the policy management module formulates various strategies —including resource management, routing, security, and access point selection

policies—based on network status and request information collected and fed back from the control layer; the query module handles queries related to access authentication based on user request information, including link status and authentication functions; and the authentication module manages multiple access authentication services, including normal, anonymous, concurrent, and broadcast authentication services.

The **control layer** comprises ground controllers and space controllers. Ground controllers include user controllers and gateway controllers that perform user access authentication-related control operations. Space controllers are primarily satellite controllers responsible for collecting space network status and satellite state information, including network bandwidth, transmission delay, packet loss rate, signal strength, online time, and satellite storage and computing capabilities.

The **device layer** includes ground forwarding devices and space forwarding devices. Ground forwarding devices—such as switches, routers, and gateways —forward and process ground data information, including user requests and satellite response information. Space forwarding devices—including medium and low Earth orbit satellites and aircraft—forward relevant information in space, including access request and response information. The device layer collects relevant data and transmits it to the authentication layer through the control layer, which formulates policies based on controller-collected information and implements policy distribution and enforcement through the control layer.

Based on the space-ground integration network composition characteristics and the proposed SDN-based access authentication architecture, the architectural topology is designed as shown in [Figure 4: see original paper]. The management layer entity is the management center. Due to limited on-board processing capabilities of satellites, to reduce satellite computational and storage pressure, the management center is deployed on the ground for easier deployment and maintenance. Control layer entities include two parts: first, ground controllers such as user controllers and gateway controllers, which serve dual purposes—collecting and maintaining network status, device entities, and authentication request information within their domain and transmitting this information to the management center, and controlling information forwarding according to management center policies; second, space controllers deployed in space, which function similarly to ground controllers by collecting and maintaining network and satellite information within their domain and controlling satellite information forwarding according to management center rules. Device layer entities primarily include ground switches, routers, and gateways, as well as space backbone and access satellites, which forward authentication requests, response information, and other data. The three layers cooperate to complete access authentication for the space-ground integration information network.

Leveraging the SDN principle of control-data plane separation, integrating SDN with space-ground integration information networks enables unified user access authentication. Controllers centrally collect network and entity status infor-

mation and control information forwarding. Various authentication services—such as anonymous and concurrent authentication—and policy management are unified under centralized management center control. SDN introduction makes space-ground integration information network usage and control more flexible, enabling automated network deployment, reducing network failure probability, and more importantly, achieving integrated utilization of network computing and storage resources to provide on-demand services for users.

2.3 SDN-Based Space-Ground Integration Information Network Access Authentication Process

Based on the proposed three-layer architecture and its topology, the access authentication method targets both wired and wireless users. The process proceeds as follows:

a) A normal user sends an access request to the relevant switch. If the switch contains the corresponding forwarding flow table, it forwards according to the flow table rules; otherwise, it forwards the request to the corresponding controller, which then sends the information to the management center, as shown by path — — in [Figure 4: see original paper].

b) Upon receiving the access request, the management center formulates appropriate routing, security, and access point selection policies based on space network status and satellite state information sent by satellite controllers, and distributes these policies to the corresponding satellite controllers, user controllers, and gateway controllers.

c) Each controller distributes policies to corresponding forwarding devices. The user' s request information follows the specified path through switches and routers to the gateway according to management center policies. After the gateway completes ground-to-space protocol conversion, the information is sent to the designated access satellite. The destination satellite performs access authentication upon receiving the request information, as shown by path — — — — — in [Figure 4: see original paper].

d) Upon successful authentication, the satellite returns a response message along the specified path (— — — — — — in [Figure 4: see original paper]). After protocol conversion from space to ground at the gateway, the message is transmitted through routers and switches to the user, who completes authentication upon receipt.

Wireless terminal users can communicate directly with satellites or follow the same authentication process as normal users. However, when the satellite requested by a wireless terminal user is out of range, the request can be sent to the management center, which controls satellites to distribute control information according to its policies, forwarding the access request to the destination access satellite via flow tables to complete the access authentication process.

3 Access Point Decision Algorithm

In the policy management module of the authentication layer, the access point selection strategy is crucial for the user access authentication process. Selecting the optimal access point can efficiently and securely satisfy user access requirements and enable rapid, secure authentication. This paper proposes an access point decision algorithm for space-ground integration information networks by combining the analytic hierarchy process (AHP) with the technique for order preference by similarity to an ideal solution (TOPSIS) [15]. The main idea is to select satellite node computing resources, storage resources, signal strength, bandwidth, transmission delay, packet loss rate, and coverage time as evaluation attributes for access point decisions. After the management center receives relevant information from controllers, it first uses a combination of logical multiplication and logical addition methods for preliminary screening to eliminate unsatisfactory solutions. Then, AHP determines the weights of each attribute, and TOPSIS identifies the ideal and negative-ideal solutions. The distances between candidate access nodes and these solutions are calculated to evaluate each scheme' s 优劣 and select the optimal access node.

3.1 Preliminary Node Screening Based on Logical Multiplication and Addition

Define the decision attribute set for satellite node i as {computing resources, storage resources, signal strength, bandwidth, transmission delay, packet loss rate, coverage time}, denoted as $S_N^i = \{CR_i, SR_i, SI_i, NB_i, TD_i, PL_i, CT_i\}$. Simultaneously define cutoff values for each attribute when a satellite node becomes an access node as $\{a', b', c', d', e', f', g'\}$. Based on whether attributes positively or negatively impact decision results, they can be classified as benefit-type or cost-type attributes. Benefit-type attributes (where larger values yield higher evaluation) include computing resources, storage resources, signal strength, bandwidth, and coverage time. Cost-type attributes (where lower values yield higher evaluation) include transmission delay and packet loss rate. When benefit-type attribute values are not lower than their corresponding cutoff values and cost-type attribute values are not higher than their corresponding cutoff values, the satellite node is added to the candidate set S'_N. Otherwise, a re-evaluation occurs with new thresholds $\{a'', b'', c'', d'', e'', f'', g''\}$. If any node attribute value is better than its threshold, the node is added to candidate set S'_N. The algorithm is as follows:

Select(S_N) =
  if ($CR_i \geq a'$ and $SR_i \geq b'$ and $SI_i \geq c'$ and $NB_i \geq d'$
    and $TD_i \leq e'$ and $PL_i \leq f'$ and $CT_i \geq g'$)
    then add S_N^i to S'_N
  elseif ($CR_i \geq a''$ or $SR_i \geq b''$ or $SI_i \geq c''$ or $NB_i \geq d''$
    or $TD_i \leq e''$ or $PL_i \leq f''$ or $CT_i \geq g''$)
    then add S_N^i to S'_N

3.2 Attribute Weight Determination Based on Analytic Hierarchy Process

After determining the preliminary solution set using logical multiplication and addition, AHP is employed to determine attribute weights for each access node.

a) **Construct the Decision Matrix.** To facilitate ranking the importance of each decision attribute for access nodes, the decision matrix is constructed based on Saaty's [16] relative importance scale between attributes, as shown in Equation (1):

$$A = [a_{ij}]_{n\times n} = \begin{bmatrix} \frac{CR}{CR} & \frac{CR}{SR} & \frac{CR}{SI} & \frac{CR}{NB} & \frac{CR}{TD} & \frac{CR}{PL} & \frac{CR}{CT} \\ \frac{SR}{CR} & \frac{SR}{SR} & \frac{SR}{SI} & \frac{SR}{NB} & \frac{SR}{TD} & \frac{SR}{PL} & \frac{SR}{CT} \\ \frac{SI}{CR} & \frac{SI}{SR} & \frac{SI}{SI} & \frac{SI}{NB} & \frac{SI}{TD} & \frac{SI}{PL} & \frac{SI}{CT} \\ \frac{NB}{CR} & \frac{NB}{SR} & \frac{NB}{SI} & \frac{NB}{NB} & \frac{NB}{TD} & \frac{NB}{PL} & \frac{NB}{CT} \\ \frac{TD}{CR} & \frac{TD}{SR} & \frac{TD}{SI} & \frac{TD}{NB} & \frac{TD}{TD} & \frac{TD}{PL} & \frac{TD}{CT} \\ \frac{PL}{CR} & \frac{PL}{SR} & \frac{PL}{SI} & \frac{PL}{NB} & \frac{PL}{TD} & \frac{PL}{PL} & \frac{PL}{CT} \\ \frac{CT}{CR} & \frac{CT}{SR} & \frac{CT}{SI} & \frac{CT}{NB} & \frac{CT}{TD} & \frac{CT}{PL} & \frac{CT}{CT} \end{bmatrix}$$

b) **Consistency Test of the Attribute Decision Matrix.** To determine whether the decision matrix is reasonable, relevant parameters must be introduced for consistency testing. The consistency ratio CR serves as the metric for testing matrix consistency, defined as the ratio of the consistency index CI to the random index RI for matrices of the same order, as shown in Equations (2) and (3):

$$CR = \frac{CI}{RI}$$

$$CI = \frac{\lambda_{\max} - n}{n-1}$$

where $\lambda_{\max}$ is the maximum eigenvalue of matrix A and n is the order of matrix A. The RI values are given in reference [15]. If $CR < 0.1$, the elements in matrix A are considered sufficiently consistent and the matrix passes the test. If $CR > 0.1$, the elements lack consistency and the matrix fails, requiring

adjustment of element values until it passes. Alternatively, CR can be calculated from $\lambda_{\max}$ and RI values as:

$$CR = \frac{\lambda_{\max} - n}{(n-1) \cdot RI}$$

If $CR > 0.1$, matrix elements must be adjusted; otherwise, matrix A passes the consistency test.

c) **Solve Attribute Weights Using the Eigenvector Method.** After the decision matrix A passes the consistency test, the eigenvector ω (i.e., the weight of each attribute) can be obtained using Equation (4):

$$A\omega = \lambda_{\max}\omega$$

3.3 Access Node Selection Based on TOPSIS Method

After determining attribute weights using AHP, TOPSIS is employed to rank access nodes and select the optimal node.

a) **Normalize the Decision Matrix.** Normalize each element of the decision matrix using Equation (5) to obtain the new matrix $B = [b_{ij}]_{m\times n}$:

$$b_{ij} = \frac{a_{ij}}{\sqrt{\sum_{i=1}^{m} a_{ij}^2}}, \quad i = 1, 2, \ldots, m; \quad j = 1, 2, \ldots, n$$

b) **Form the Weighted Normalized Matrix.** Process the normalized matrix B using the weight vector $\omega = (\omega_1, \omega_2, \ldots, \omega_n)^T$ obtained from AHP to form the weighted normalized matrix $C = [c_{ij}]_{m\times n}$ using Equation (6):

$$c_{ij} = b_{ij} \cdot \omega_j, \quad i = 1, 2, \ldots, m; \quad j = 1, 2, \ldots, n$$

c) **Determine the Ideal and Negative-Ideal Solutions.** Based on the cardinal information in the decision matrix, establish the ideal solution x^+ and negative-ideal solution x^-. The ideal solution is determined by Equation (7), and the negative-ideal solution by Equation (8):

$$x_j^+ = \begin{cases} \max_i c_{ij}, & \text{if } j \in \{CR, SR, SI, NB, CT\} \\ \min_i c_{ij}, & \text{if } j \in \{TD, PL\} \end{cases}$$

$$x_j^- = \begin{cases} \min_i c_{ij}, & \text{if } j \in \{CR, SR, SI, NB, CT\} \\ \max_i c_{ij}, & \text{if } j \in \{TD, PL\} \end{cases}$$

d) **Calculate Distances to Ideal and Negative-Ideal Solutions.** The distance between access node i and the ideal solution is given by Equation (9), and the distance to the negative-ideal solution by Equation (10):

$$d_i^+ = \sqrt{\sum_{j=1}^{n}(c_{ij} - x_j^+)^2}, \quad i = 1, 2, \ldots, m$$

$$d_i^- = \sqrt{\sum_{j=1}^{n}(c_{ij} - x_j^-)^2}, \quad i = 1, 2, \ldots, m$$

e) **Calculate Comprehensive Evaluation Parameter EI for Ranking.** The EI value is calculated using Equation (11). A larger EI indicates better comprehensive performance and greater suitability for user access:

$$EI_i = \frac{d_i^-}{d_i^+ + d_i^-}, \quad i = 1, 2, \ldots, m$$

3.4 Access Point Selection and Handover Process

When a user first accesses the space-ground integration information network, access information is sent through switches and controllers to the management center. The management center runs the proposed access point selection algorithm using collected satellite and network status information to formulate policies, which are then distributed to user satellites for optimal access point selection. When the access point changes, the request information is resent through controllers to the management center, which obtains the latest real-time network status information, reformulates policies, and distributes them. The specific process is shown in [Figure 5: see original paper].

4.1 Calculation Methods for Access Node Decision Attribute Values

Before experimental simulation, data must be obtained, with each attribute value calculated using appropriate methods. Using OPNET simulation software to obtain access node attribute information, each attribute is calculated as follows:

Computing Resources: Generally reflected in memory and CPU capacity. More remaining memory, faster memory access speed, higher CPU frequency and word length, larger cache, and lower CPU utilization rate indicate more abundant computing resources. The calculation method is shown in Equation (12):

$$CR = \frac{M \cdot r_{ws} \cdot f_{CPU} \cdot W_{CPU} \cdot C_{CPU}}{U_{CPU}}$$

where M represents remaining memory, r_{ws} represents memory access speed, f_{CPU} represents CPU frequency, W_{CPU} represents word length, C_{CPU} represents CPU cache, and U_{CPU} represents CPU utilization.

Storage Resources: Generally reflected in disk read/write speed, remaining storage space, disk cache, disk rotation speed, average access time, and queue length. Equation (13) captures these factors:

$$SR = \frac{r_{ws} \cdot S_s \cdot C_{cache} \cdot D_s}{D_{at} \cdot Q_s}$$

where r_{ws} represents disk read/write speed, S_s represents remaining storage space, C_{cache} represents disk cache, D_s represents disk rotation speed, D_{at} represents average access time, and Q_s represents disk queue length.

Signal Strength: Varies with environmental interference. Equation (14) reflects signal strength over time:

$$SI = 0.2 \times SI_{old} + 0.8 \times SI_{new}$$

where SI_{old} is the previously obtained signal strength and SI_{new} is the currently obtained signal strength.

Bandwidth: Can be represented by bandwidth idle rate over a period, as shown in Equation (15):

$$NB = \frac{\int_0^t (B_{max} - B_{use})\, dt}{B_{max} \cdot t}$$

where B_{max} represents maximum bandwidth, B_{use} represents used bandwidth, and t represents time.

Transmission Delay: Calculated using Equation (16):

$$TD = \frac{s}{v}$$

where s represents the distance between user and access node, and v represents electromagnetic wave transmission speed.

Packet Loss Rate: Calculated using Equation (17):

$$PL = \frac{P_{in} - P_{out}}{P_{in}}$$

where P_{in} and P_{out} represent input and output data, respectively, indicating the proportion of lost packets among transmitted packets.

Coverage Time: Calculated using position vector information between access node and user. Compute the angle φ between satellite and user, with the visibility function as $\phi = 90^\circ - \varphi - \alpha$, where α is the user' s required elevation angle to the access node. When ϕ is positive, user and access node can communicate. Using this, the maximum communication angle can be calculated, and combined with access node movement speed and direction information, coverage time can be determined.

4.2 Experiments on SDN-Based Space-Ground Integration Information Network Access Point Selection Algorithm

Based on the calculation methods in Section 4.1, attribute values for each node are obtained and filtered using the preliminary screening algorithm from Section 3.1. Due to different meanings and significant numerical differences among indicators, TOPSIS is used to normalize the decision matrix for intuitive decision-making. The attribute values for candidate access nodes are shown in .

Table 1: Candidate Access Node Attribute Values

Name	Computing Resources	Storage Resources	Signal Strength	Bandwidth	Transmission Delay	Packet Loss Rate	Coverage Time
N1	0.1228	0.0386	0.0987	0.0243	0.0180	0.0220	0.1093
N2	0.0671	0.0134	0.0370	0.0104	0.0809	0.0469	0.0923
N3	0.1055	0.0218	0.0863	0.0139	0.0904	0.0323	0.0996
N4	0.1151	0.0269	0.0493	0.0174	0.0539	0.0264	0.0972
N5	0.0440	0.0323	0.0996	0.0323	0.0996	0.1151	0.0269
N6	0.0493	0.0174	0.0539	0.0264	0.0972	0.0440	0.0323

The decision matrix is constructed using AHP as shown in Equation (18). MATLAB calculates the maximum eigenvalue $\lambda_{\max} = 7.1825$, yielding the consistency ratio $CR = 0.0230 < 0.1$, which passes the consistency test. The eigenvector method solves for attribute weights:

$$\omega = [0.2483, 0.0686, 0.1740, 0.0427, 0.1351, 0.0831, 0.2483]^T$$

After normalization, the weighted normalized matrix C is formed as shown in Equation (19). The ideal solution x^+ and negative-ideal solution x^- are then calculated based on the matrix:

$$x^+ = (0.1228, 0.0386, 0.0987, 0.0243, 0.0180, 0.0220, 0.1093)$$

$$x^- = (0.0671, 0.0134, 0.0370, 0.0104, 0.0809, 0.0469, 0.0923)$$

The distances d_i^+ from each optional access node to the ideal solution and d_i^- to the negative-ideal solution are calculated, and the comprehensive evaluation parameter EI is computed. The results are shown in .

Table 2: Distances to Ideal Solution and Comprehensive Evaluation Parameter Values

Node	d_i^+	d_i^-	EI_i
N1	0.0671	0.0202	0.231
N2	0.0987	0.0209	0.175
N3	0.0180	0.0337	0.652
N4	0.1020	0.0921	0.474
N5	0.0134	0.0740	0.847
N6	0.0243	0.0719	0.747

The access node ranking based on EI is: $N_5 > N_6 > N_3 > N_4 > N_1 > N_2$. Node N_5 has the highest comprehensive evaluation index, making it the optimal choice for access.

5 Conclusion

This paper proposes an SDN-based access authentication architecture and method for space-ground integration information networks. After introducing the basic composition and architecture of space-ground integration information networks, a novel access authentication architecture is proposed by integrating SDN, with detailed description of its authentication process. Subsequently, according to the characteristics of the software-defined space-ground integration information network, an access point selection algorithm is proposed by combining AHP with TOPSIS. Simulation results demonstrate the algorithm' s effectiveness in meeting space-ground network access authentication requirements. Future work will focus on actual simulation deployment and implementation of the proposed SDN-based space-ground integration network access authentication architecture and method.

References

[1] Li Fenghua, Yin Lihua, Wu Wei, et al. Research progress and development trends of space-ground integration information network security technologies [J]. Journal on Communications, 2016, 37(11): 156-168.

[2] Wang Chunfeng. Research on software-defined reconfigurable satellite network systems [J]. Journal of China Academy of Electronics and Information Technology, 2015, 10(5): 455-459.

[3] Chen Chen, Xie Shanshan, Zhang Xiaoxiao, et al. A new generation of space-air-ground integrated network architecture with aggregated SDN control [J]. Journal of China Academy of Electronics and Information Technology, 2015, 10(5): 450-454.

[4] Iqbal H, Ma J, Stranc K, et al. A software-defined networking architecture for aerial network optimization [C]// Proc of IEEE Netsoft Conference and Workshops. 2016: 151-155.

[5] Li Ting, Hu Jianping, Xu Huizhong. Analysis of software-defined networking applications in space-based information networks [J]. Telecommunication Engineering, 2016, 56(3): 259-266.

[6] Wu Manqing, Wu Wei, Zhou Bin, et al. Overall architecture concept for space-ground integration information network [J]. Satellite & Network, 2016(3): 30-36.

[7] Stanford University. Clean slate program [EB/OL]. (2017-05-25) [2017-10-09]. https://en.wikipedia.org/wiki/Clean_Slate_Program.

[8] MCKEOWN N. Software-defined Networking [J]. China Communications, 2009, 11(2): 1-2.

[9] Wang Mengmeng, Liu Jianwei, Chen Jie, et al. Software-defined networking: Security models, mechanisms, and research progress [J]. Journal of Software, 2016, 27(4): 969-992.

[10] Wang K, Wang Y, Zeng D, et al. An SDN-based architecture for next-generation wireless networks [J]. IEEE Wireless Communications, 2017, 24(1): 25-31.

[11] Costa-Perez X, Garcia-Saavedra A, Li X, et al. 5G-crosshaul: an SDN/NFV integrated Fronthaul/Backhaul transport network architecture [J]. IEEE Wireless Communications, 2017, 24(1): 38-45.

[12] Rahman M M, Despins C, Affes S. Design optimization of wireless access virtualization based on cost & QoS trade-off utility maximization [J]. IEEE Trans on Wireless Communications, 2016, 15(9): 6146-6162.

[13] Callegati F, Cerroni W, Contoli C, et al. SDN for dynamic NFV deployment [J]. IEEE Communications Magazine, 2016, 54(10): 89-95.

[14] ADAMI D, MARTINI B, SGAMBELLIRI A, et al. An SDN orchestrator for cloud data center: System design and experimental evaluation [J]. Transactions on Emerging Telecommunications Technologies, 2017(11): e3172.

[15] Yue Chaoyuan. Decision Theory and Methods [M]. Beijing: Science Press, 2003.

[16] Yan Chongchong, Hao Yongsheng. Aerial target threat estimation based on analytic hierarchy process (AHP) [J]. Computing Technology and Automation, 2011, 30(2): 118-121.

Note: Figure translations are in progress. See original paper for figures.