Secure East-West Communication to Approve Service Access Continuity for Mobile Devices in a Distributed SDN

Maroua Moatemri[1,2(✉)], Hamdi Eltaief[1,2], Ali El Kamel[1,2], and Habib Youssef[1,2]

[1] University of Sousse, Khalifa Karoui Street Sahloul 4 Sousse, Sousse, Tunisia
hamdi.eltaief@issatso.rnu.tn, Habib.youssef@fsm.rnu.tn
[2] PRINCE Research Lab. ISITC Hammam Sousse, Sousse, Tunisia
{maroua.moatemri,ali.kamel}@isitc.u-sousse.tn

Abstract. In a distributed mobile Software Defined Mobile Network (SDMN), a device is in a continuous movement from one domain to another. Since a different controller is responsible for each domain, the devices' authentication information needs to be communicated between the SDN controllers (this type of communication is called East-West communication) to ensure the continuity access to the used devices services. This paper proposes a new secure East-West communication to approve service access continuity for mobile devices in a Distributed SDN. A comparative study between the VPN based approach and the proposed one is done both analytically and by simulation according to two criteria: the approval access authentication delay and the communication overhead. The results show that the proposed approach provides a secure East-West communication using less communication overhead and decreases the approval access authentication delay of mobile devices in an SDN.

Keywords: Service access continuity · SDN · Security · East-west communication · Approval access authentication delay

1 Introduction

Software Defined Network is a network paradigm defined by the physical separation of the control plane and the data plane of a network [5]. A distributed SDN is composed with numerous controllers and every controller is responsible of a different domain. To be able to apply the SDN paradigm to wireless mobile networks, SDMN has been defined. In fact, SDMN is an extension due to the addition of mobile networks' special functions [3]. It presents multiple advantages compared to regular mobile network such as flexibility, centralized control and reduction of the backhaul device operating cost [3]. In the recent years, network services are becoming more and more time sensitive. In a

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2022
O. Gervasi et al. (Eds.): ICCSA 2022, LNCS 13375, pp. 283–297, 2022.
https://doi.org/10.1007/978-3-031-10522-7_20

distributed SDN, any mobile device must have access to the service while moving from one domain to another. In this context, his authentication information needs to be communicated between the SDN controllers in a minimal time. On the other hand, this information is considered extremely sensitive, so they must be communicated in a secure environment. In this paper, we propose a new secure east-west communication approach to approve service access continuity for mobile devices in a distributed SDN. The proposed solution provides the security basics (confidentiality, integrity, and authentication) in order to protect the users' authentication information communicated between the different controllers. It also minimizes the time needed to approve the continuity of the access to the service in order to not affect the QoS. The rest of this paper is organized as follow. The next section presents a brief overview of the background and related work about multi controller SDN and the protocols that could be used to protect the SDN east-west communications. Section 3 defines the proposed east-west communication approach to approve service access continuity for mobile devices in a distributed SDN. The analytical and experimental evaluations are presented in Sect. 4. Section 5 concludes this paper.

2 Background and Related Work

In a traditional SDN, only one controller is used to manage all the network. This will present a limitation in terms of scalability. In fact, with the continuous evolution of the network demands, a single controller will not be able to manage an entire network due to its limited capacity. Another problem that a single controller SDN encounter is the single point of failure. In order to overcome these issues, the use of multi-controller SDN have been proposed [9]. When using a multi-controller SDN, several architectures could be adopted. The first, is the flat architecture, composed with various domains and every controller manages one domain. The second architecture is the hierarchical architecture. It is tree like architecture using different layers of controllers. Most solutions propose a two layer controller architecture. The domain controllers which handle switches in their domains and a root controller that keeps a global view of the network and manage the domain controllers [9]. Another design of architecture that could be adopted is the hybrid architecture [20]. It is a two layer architecture composed with multiple root controllers and each one manages a few domain controllers. To secure the east west communications in a distributed SDN, a few ways have been proposed. Jun-Huy Lam et al. [13] suggest using Identity-Based Cryptography (IBC) for this purpose. IBC protocol has been introduced in 1984 by Adi Shamir [21]. It is based on the generation of the users' private keys through their unique identities via a trusted third party called the Private Key Generator (PKG). However, using this protocol require a secure channel to exchange data between the PKG and the users [2]. Another problem due to

the use of the IBC is that if the PKG is compromised then all the messages that had been signed by the keys generated by it are also compromised. In [8], the use of both TLS[19] and IPsec [10–12,15,17] protocols has been proposed to secure SDN's east west communications. With the use of TLS, many problems will be encountered. First, if we have different communication scenarios, which is the case in our scenario, we cannot implement different security policies [18]. Second, TLS is not capable of providing the data origin authentication which will cause problems since it is one of the most important security services to guarantee in a network. As for the IPsec, its first problem is that it needs a lot of communications for the users' authentication. Also, another disadvantage of the IPsec is due to the use of the tunneling mode which will cause bandwidth problems.

3 The Proposed Approach to Approve Service Access Continuity for Mobile Devices in a Distributed SDN

3.1 Overview and Motivation

The main idea of our approach consists of centralizing the authentication information of all the network users. Thus, when a new mobile device enters in the domain of a foreign controller, it will need his authentication information to authenticate it. To do so, the foreign controller sends the device's authentication information (user profile, attributes, master session key, time stamp...)[1] to the network administrator through the shortest path. If the user is registered, then, the network administrator responds with a confirmation message through the same path. In that case, it will grant its access to the service. Compared to the VPN authentication method, the proposed approach presents several advantages. First, using the VPN based approach requires the use of a new VPN channel for each communication between two controllers. This will make using this method on large scale networks not possible due to the resource limitation. This will as well introduce a heavy network load which will lead to bandwidth problems. Secondly, since the authentication information is centralized, they will not be shared between all the controllers. This will decrease the risk that an intruder steals and uses this critical data. The proposed architecture is presented in Fig. 1.

3.2 Security Analysis

Some of the users' authentication information such as the master session key are critical and needs to be protected against some malicious attacks. In our approach, three different communication types are proposed. The first type is the "Controller-Controller" communications. In this type, the authentication information data will only be accessible by the end devices. Thus, the intermediate controllers will only play the simple role of data routing. The second type is the

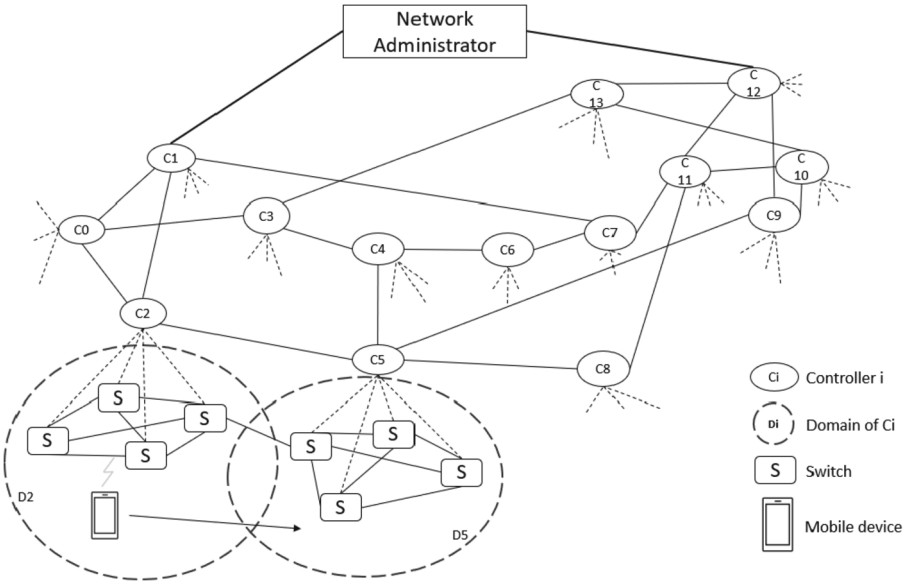

Fig. 1. The proposed architecture

communications "Controller-Network administrator". In this type, the authentication information data will pass through an exterior network. In this case, the confidentiality is required so the critical data will not be intercepted. Also, the network administrator must be sure that the message from the controller C_i is authentic, and that the data has not been modified. To ensure that, we must guarantee the source authentication and the data integrity. The last communication type is the "Network administrator-Controller" communication. This communication is nothing more than a simple acknowledgment that will allow the controller to approve service access continuity for the mobile device. In that case, the confidentiality is not required since the data sent is not critical. Contrariwise, the source authentication and the data integrity are very important because the controller must be sure that the response did truly come from the network administrator and that it has not been modified during the data transfer.

3.3 Conduct of the Proposed Approach

The proposed approach has two different phases: the first is an offline phase and the second is online.

The Offline Phase: Pre-Establishment. This first phase aims to set up the network. Several tasks will take place offline:

Keys Distribution. The network administrator and all the controllers will have a public key and a private key. The notation of the different keys is presented in the Table 1.

Table 1. Keys' description.

Notation	Representation
K_{admin}^{-1}	The network administrator's private key
K_{admin}	The network administrator's public key
K_{Ci}^{-1}	The controller i private key
K_{Ci}	The controller i public key

Keys' Exchange. The network administrator and the controllers make their public keys available for all the other network elements [7].

Protocol Hello. Used by the controllers to discover the network.

Shortest Path Selection. The shortest path is used to send the user's authentication information. For this task, the OSPF protocol [16] is used.

Switches' Establishment. Using the proposed approach to improve switch-to-controller assignment [4].

Users' Registration on the Network. To benefit from a service, the user needs to join the network through a challenge-response authentication [1].

Send the Users' Authentication Information to the Network Administrator. Every controller needs to send the authentication information of his users to the network administrator.

The Online Phase, Now that the network is set up, it will start functioning. The scenario is as follow: When a mobile device moves from his source domain to foreign domain, the access authentication approval process will star and presented as follow:

Step 1: The mobile device asks for approval to access to the service. It sends its authentication information to the foreign controller.
The following notation is used to express the communication between controllers in the next steps.

M_i: Plaintext authentication information message sent by the controller C_i
M_s: Encrypted message
C_i : Foreign controller's identity
admin : Network administrator's identity
N : Sequence number
H : Hash function
m : Plaintext acknowledgement message
admin : Network administrator's identity
N : Sequence number
m_s : Acknowledgement message sent by admin

Step 2: The foreign controller sends the authentication information to the network administrator. To ensure the confidentiality of M_i, C_i encrypts M_i with the administrator's public key.

$$C_i \rightarrow admin : M_s = \Big\{ M_i, N, C_i, admin, \big\{ H\big(M_i, N, C_i, admin\big) \big\}_{K_{Ci}^{-1}} \Big\}_{K_{admin}}$$

Step 3: The network administrator decrypts the message using its own private key.

$$admin : M_i', N', C_i', admin', \big\{ H\big(M_i, N, C_i, admin\big) \big\}_{K_{Ci}^{-1}} = \big\{ M_s \big\}_{K_{admin}^{-1}}$$

Step 4: To ensure the identity and the message are from the claimed controller Ci, the network administrator needs to be able to decrypt the message digest using the controller's public key (K_{Ci}).

$$H\big(M_i, N, C_i, admin\big) = \Big\{ \big\{ H\big(M_i, N, C_i, admin\big) \big\}_{K_{Ci}^{-1}} \Big\}_{K_{Ci}}$$

Step 5: To make sure that the message has not been altered, the network administrator computes the received message digest through the same hush function H. If,

$$H\big(M_i', N', C_i', admin'\big) = H\big(M_i, N, C_i, admin\big),$$

then the message has not been altered.

Step 6: If the user is subscribed to the service, then the network administrator sends an acknowledgement message to the controller C_i to approve the access.

$$admin \rightarrow C_i : m_s = m, N, admin, C_i, \big\{ H\big(m, N, admin, C_i\big) \big\}_{K_{admin}^{-1}}$$

Step 7: The controller decrypts the message digest using the network administrator's public key to ensure the identity and the message are from the claimed network administrator.

$$\big\{ m_s \big\}_{K_{admin}} = \Big\{ m, N, admin, C_i, \big\{ H(m, N, admin, C_i) \big\}_{K_{admin}^{-1}} \Big\}_{K_{admin}}$$

Step 8: The controller computes the received message digest through the same hush function H. If

$$H\left(m', N', C_i', admin'\right) = H\left(m, N, C_i, admin\right),$$

then the message has not been altered.

Step 9: The controller saves the information to allow the user to access the service during the intra-domain movement for the same session. These different steps are represented in the diagram of the Fig. 2.

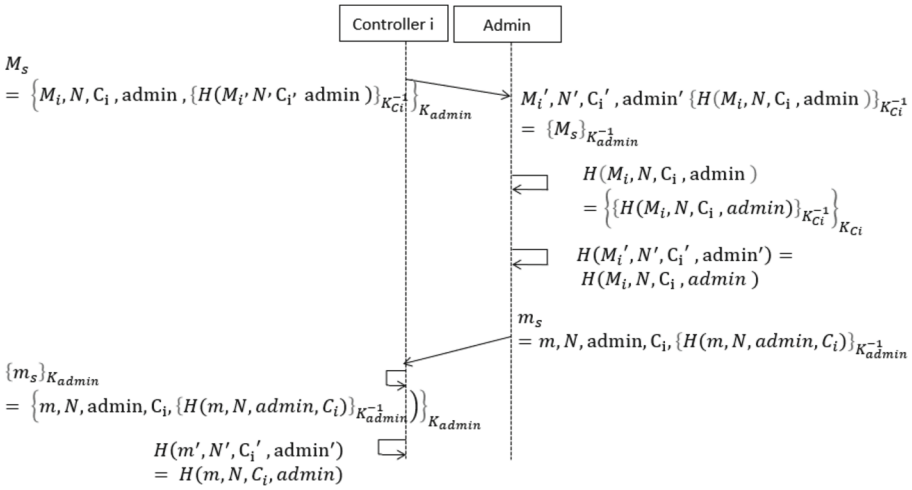

Fig. 2. Controller-Network administrator communications

4 Evaluation

The proposed approach is evaluated based on an analytical and experimental study according to two criteria: the approval access authentication time and the communication overhead.

4.1 Analytical Evaluation

Notation. During this section, the notation used is presented in the Table 2.

Table 2. Analytical evaluation notation.

Symbol	Representation
HC	Home or source controller
VC	Visitor or foreign controller
Ck	The border controller (C1 or C12)
NA	Network administrator
$T^{prop}_{ACAS}(VC, NA)$	Time to approve the continuity of the access to the service using the proposed method
$T^{vpn}_{ACAS}(VC, HC)$	Time to approve the continuity of the access to the service using the VPN based approach
$Com_{(Ci,Cj)}$	Communication cost between two neighbor controllers
$Com_{(Ck,NA)}$	Communication cost between the network administrator and a controller that is directly linked to the network administrator
P	Shortest path between the source (HC) and the destination (VC)
Pa	Shortest path between the VC and Ck
T_{prop}	Propagation time
T_{em}	Emission time
T_{cal}	The total time for encryption, decryption, hash,
V_{prop}	Propagation velocity
$T_{trans(request)}$	Time required for the request to be transmitted from the VC to the HC
$T_{trans(reply)}$	Time required for the reply to be transmitted from the HC to the VC
$T_{request}$	Time required for the request to attend the network administrator through the shortest path
$T_{response}$	Time required for the acknowledgement to attend the controller through the shortest path
$size_{req}$	Size of the message of the request
$size_{reply}$	Size of the message of the acknowledgement
$datarate$	Transmission speed

Analytical Evaluation of the VPN Based Approach

Approval Access Authentication Delay. Knowing the source controller, the time to approve the continuity of the access to the service by the foreign controller is expressed using the Eq. 1

$$T^{vpn}_{ACAS}(VC, HC) = T_{trans(request)} + T_{trans(reply)} + T_{Cal} \quad (1)$$

The communication cost between two neighbor controllers Ci and Cj ($Com_{(Ci,Cj)}$) is calculated as follow in the Eq. 2

$$Com_{(Ci,Cj)} = 2 * \frac{(distance(Ci, Cj))}{V_{prop}} + \frac{(size_{req} + size_{reply})}{datarate} + T_{Cal} \quad (2)$$

The total approval access authentication cost is the sum of the costs of all the needed communications.

$$T^{vpn}_{ACAS}(VC, HC) = \sum_{(Ci,Cj)\in P} Com_{(Ci,Cj)} \tag{3}$$

$$T^{vpn}_{ACAS}(VC, HC) = \sum_{(Ci,Cj)\in P} 2*\frac{(distance(Ci, Cj))}{V_{prop}} + \frac{(size_{req} + size_{reply})}{datarate} + T_{Cal} \tag{4}$$

Communication Overhead. To protect the sent data, security protocols add to the payload an overhead that will guarantee some security services. The tunnel mode of the ESP mechanism of the IPsec protocol, that will be used to compare our approach, guarantee the following security services:

- Confidentiality: through data encryption
- Integrity and data origin authentication: through hashing and digital signature
- Reply attack protection: through the Nonce

Knowing that the AES-CBC Cipher is used for the authentication and the HMAC-SHA-256 is used for the integrity and authentication, the data packet format and the total communication overhead used are presented in Table 3.

Analytical Evaluation of the Proposed Approach

Approval Access Authentication Delay. The time to approve the continuity of the access to the service by the foreign controller is expressed using the Eq. 5

$$T^{prop}_{ACAS}(VC, NA) = T_{request} + T_{response} + T_{cal} \tag{5}$$

Table 3. Communication overhead for the used VPN based approach.

Field	Size(Bits)
Source address	32
Destination address	32
SPI	32
Sequence number	32
Padding	144
Padding length	8
Next header	8
Authentication data	256
Total communication overhead	544

The communication cost between two neighbor controllers Ci and Cj ($Com_{(Ci,Cj)}$) is calculated as in the Eq. 2.

The approval access authentication delay cost is the sum of the cost of all the needed communications to attend the border controller and the cost of the communication to attend the network administrator. This is expressed in the Eq. 6

$$T^{prop}_{ACAS}(VC, NA) = (\sum_{(Ci,Cj)\in Pa} Com_{(Ci,Cj)}) + Com_{(Ck,NA)} \tag{6}$$

$$T^{prop}_{ACAS}(VC, NA) = (\sum_{(Ci,Cj)\in Pa} 2 * \frac{(distance(Ci, Cj))}{V_{prop}} + \frac{(size_{req} + size_{reply)}}{datarate} + T_{Cal}) + 2 * \frac{(distance(Ck, NA))}{V_{prop}} + \frac{(size_{req} + size_{reply)}}{datarate} + T_{Cal} \tag{7}$$

Communication Overhead. In the proposed approach, we propose to add the following data to protect the sent data packets:

- Source Identifier: 32 bits
- Network administrator identifier: 32 bits
- Sequence number: 32 bits
- Authentication data: 256 bits (due to the use of the ECC [14])

The total size of the overhead of the proposed approach is 352 bits. This is less than the overhead added with the VPN based approach, which will generate a bandwidth gain.

4.2 Experimentation

To test the proposed approach and compare it with the VPN based approach, the NSFNET [22] network architecture is used. It is composed of 14 nodes and 21 links. The Fig. 3 presents the approximate distances between the nodes in kilometers [6]. We suppose that the network administrator is equidistant from the two controllers it is connected to.

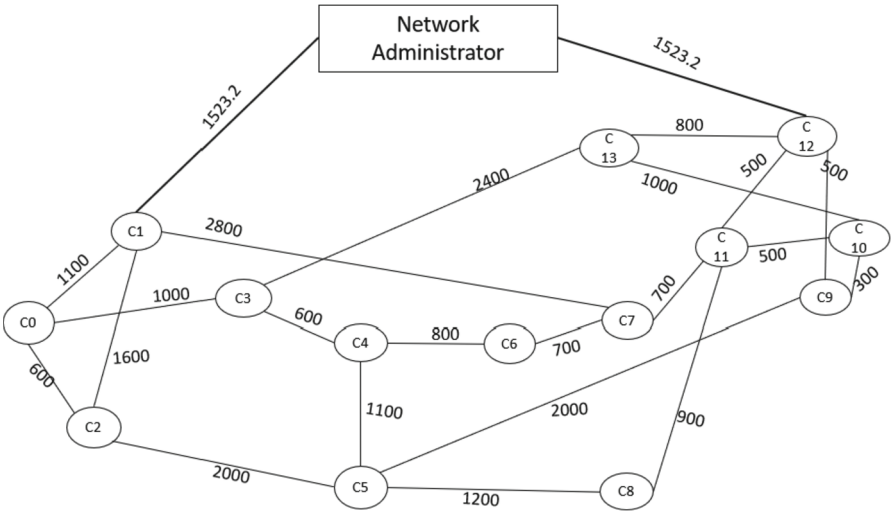

Fig. 3. The proposed architecture with approximate distances

The comparison is realized both analytically and with simulation. It is based on the approval access authentication delay using the VPN based approach and the proposed approach. The approval access authentication delay is computed using the Eq. 4 for the used VPN based approach and the Eq. 7 for the proposed approach. The route is composed with the controllers managing the domains that the mobile device visited during his movement. Since one route is composed with various foreign controllers (VCi), we will have an approval access authentication delay for each VCi. Thus, we will compare the average approval access authentication delay computed by the Eq. 8 for the VPN based approach and by the Eq. 9 for the proposed method.

$$Average\ T_{ACAS}^{vpn} = \frac{\sum_{(VCi)\in Route} T_{ACAS}^{vpn}(VCi, HC)}{(number\ of\ VCi \in Route) - 1} \tag{8}$$

$$Average\ T_{ACAS}^{prop} = \frac{\sum_{(VCi)\in Route} T_{ACAS}^{prop}(VCi, NA)}{(number\ of\ VCi \in Route) - 1} \tag{9}$$

The different scenarios are presented in the Table 4. The source node represents the node where the mobile is originally registered.

Analytical Results. The results obtained analytically presented in the Fig. 4 prove an improvement of our proposed approach in terms of average approval access authentication delay (T_{ACAS}) in most scenarios compared to the VPN based approach. Those improvements are explained by the distance optimization in the proposed approach.

Table 4. Different test scenarios.

Scenario	Source node	Route
1	11	8-5-2-0-1
2	7	7-1-0-2
3	9	7-1-0-3
4	2	8-9-10-13-12
5	13	13-1-0-2-5
6	0	0-1-7-11-12
7	0	0-1-13-12-10
8	3	3-13-12-10-9
9	7	8-5-2-0-1-7
10	10	10-13-3-2-1-0
11	5	5-9-10-12-13-1
12	13	13-1-0-2-5
13	11	8-5-2-0
14	7	8-5-2-0-1
15	9	9-7-1-0-3
16	8	8-11-12-13-1-0
17	13	13-1-3-4-5

The average delay obtained from the different scenarios in the proposed approach is of 24.18 ms compared to 31.1 ms obtained with the VPN based approach which presents an improvement of 6.9 2 ms.

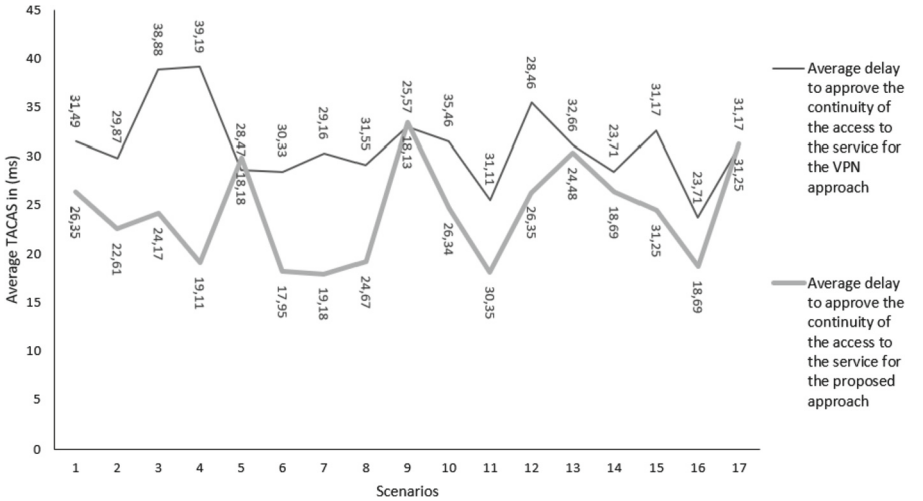

Fig. 4. Analytical comparison of the average authentication time

Experimental Results. To implement the experimental tests, we used the NS2 for simulating the network and the NAM tool to visualize the network simulations.

The computer used has 4 GB of Ram and 931 GB of hard disk size. Its processor is the Intel® Core™ i3-7020U CPU @ 2.30 GHz.

We simulated the same scenarios as those used with the analytical results. The obtained simulation results presented in the Fig. 5 validate the analytical results. The proposed approach, with an average delay of 24.19 ms generates a 6.91 ms gain compared to 31.1 ms for the classical approach.

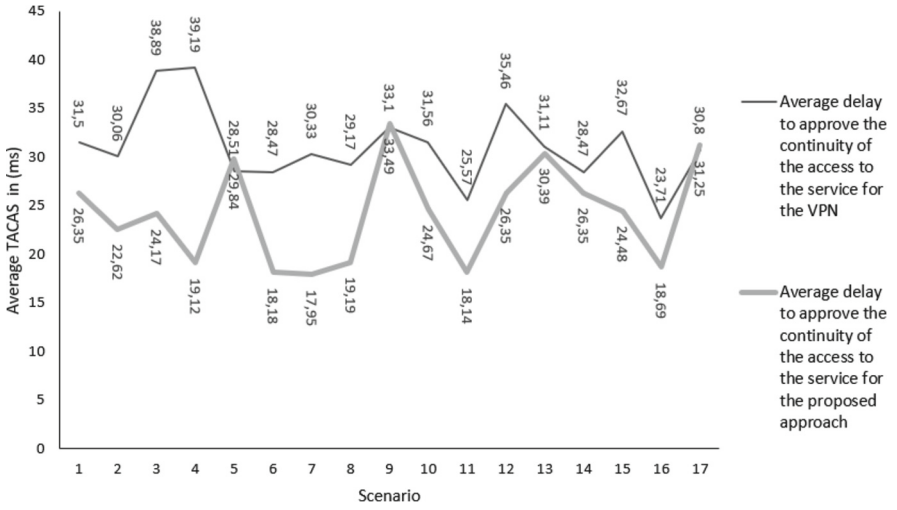

Fig. 5. Experimental comparison of the average authentication delay

5 Conclusion

The main purpose of this paper is to present a new secure east-west communication approach to approve service access continuity for mobile devices in a distributed Software Defined Network. East-west communication approaches need to provide communications' security to secure the users' authentication information. Another criterion is the approval access authentication delay that should be minimal to not negatively influence the Quality of Service (QoS). For a large scale network, our proposed approach ensure east-west communications' security to secure the users' authentication information generating a lightweight network load. The analytical and the simulation studies prove that the proposed approach presents an improvement in terms of both overhead size and approval access authentication delay compared with the used VPN based approach.

References

1. Aissaoui, H., Urien, P., Pujolle, G.: Low latency of re-authentication during handover: Re-authentication using a signed token in heterogeneous wireless access networks. In: 2013 International Conference on Wireless Information Networks and Systems (WINSYS), pp. 1–7. IEEE (2013)
2. Anand, D., Khemchandani, V., Sharma, R.K.: Identity-based cryptography techniques and applications (a review). In: 2013 5th International Conference and Computational Intelligence and Communication Networks, pp. 343–348. IEEE (2013)
3. Chen, M., Qian, Y., Mao, S., Tang, W., Yang, X.: Software-defined mobile networks security. Mob. Netw. Appl. **21**(5), 729–743 (2016)
4. El Kamel, A., Youssef, H.: Improving switch-to-controller assignment with load balancing in multi-controller software defined wan (sd-wan). J. Netw. Syst. Manag. **28**(3), 553–575 (2020)
5. Foundation, O.N.: Software-defined networking (sdn) definition. https://opennetworking.org/sdn-definition/
6. Ghose, S., Kumar, R., Banerjee, N., Datta, R.: Multihop virtual topology design in WDM optical networks for self-similar traffic. Photonic Netw. Commun. **10**(2), 199–214 (2005)
7. Hendaoui, F., Eltaief, H., Youssef, H.: A collaborative key management scheme for distributed smart objects. Trans. Emerg. Telecommun. Technol. **29**(6), e3198 (2018)
8. Hettiarachchi, S.: Securing east-west communication in clustered multi-sdn controller network (2018)
9. Hu, T., Guo, Z., Yi, P., Baker, T., Lan, J.: Multi-controller based software-defined networking: a survey. IEEE Access **6**, 15980–15996 (2018)
10. Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., Kivinen, T.: Internet key exchange protocol version 2 (ikev2). Technical report, RFC 5996 (2010)
11. Kent, S., Atkinson, R.: Ip encapsulating security payload (esp): Rfc 4303 (proposed standard) (2005)
12. Kent, S., Header, I.A.: Rfc 4302. IETF (2005)
13. Lam, J.H., Lee, S.G., Lee, H.J., Oktian, Y.E.: Securing distributed SDN with IBC. In: 2015 Seventh International Conference on Ubiquitous and Future Networks, pp. 921–925. IEEE (2015)
14. Langley, A., Hamburg, M., Turner, S.: Elliptic Curves for Security. RFC 7748 (2016). https://doi.org/10.17487/RFC7748, https://rfc-editor.org/rfc/rfc7748.txt
15. Maughan, D., Schertler, M., Schneider, M., Turner, J.: Internet security association and key management protocol (ISAKMP) (1998)
16. Moy, J.: Rfc2328: Ospf version 2 (1998)
17. Orman, H.: The oakley key determination protocol rfc 2412. IETF, Freemont, CA (1998)
18. Qin, H., Wang, N.: A data-origin authentication protocol based on ONOS cluster. In: MATEC Web of Conferences. vol. 56, p. 01006. EDP Sciences (2016)
19. Rescorla, E., Dierks, T.: The transport layer security (TLS) protocol version 1.3 (2018)
20. Sarmiento, D.E., Lebre, A., Nussbaum, L., Chari, A.: Decentralized SDN control plane for a distributed cloud-edge infrastructure: a survey. IEEE Commun. Surv. Tutor. **23**, 256281 (2021)

21. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_5
22. Tomovic, S., Radonjic, M., Radusinovic, I.: Bandwidth-delay constrained routing algorithms for backbone SDN networks. In: 2015 12th International Conference on Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS), pp. 227–230 (2015). https://doi.org/10.1109/TELSKS.2015.7357775