IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 10, 2019, accepted September 2, 2019, date of publication September 12, 2019, date of current version September 26, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2941084

A Lightweight Two-Way Authentication Scheme Between Communication Nodes for Software Defined Optical Access Network

YONGLI TANG, TAO LIU, XU HE, JINXIA YU, AND PANKE QIN
School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454003, China

Corresponding author: Panke Qin (qinpanke@hpu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61802117, in part by the "13th Five-Year" National Crypto Development Foundation under Grant MMJJ20170122, in part by the Projects of Henan Provincial Department of Education under Grant 18A413001, and in part by the Doctoral Scientific Fund of Henan Polytechnic University under Grant B2016-36.

ABSTRACT For the rapid increase in the number of optical line terminals (OLTs) and optical network units (ONUs) connected to the control center in the software defined optical access network (SDOAN) environment, the security problems caused by the communication between devices and the high cost caused by the introduction of security schemes, we propose a lightweight identity two-way authentication scheme (LTWA) based on the cryptographically generated address (CGA) algorithm combined with the hash generated address (HGA) algorithm. The scheme introduces the CGA algorithm and the HGA algorithm without third party participation, so as to complete the first authentication binding and the non-first authentication binding between the communication nodes respectively, which effectively prevents an attacker from forging or tampering with authentication interaction messages, thereby establishing an end-to-end trusted connection in the access network. We experimentally verify the proposed LTWA scheme. The simulation results show that the scheme guarantees the security interaction between communication nodes, and reduces the average computational overhead and the blocking rate caused by malicious attacks.

INDEX TERMS Authentication, openflow, optical access network, OLT, SDN.

I. INTRODUCTION

With the rapid increase in the number of network users, some issues are awaiting to be addressed. For example, the problem of the increased operation and maintenance cost due to the geographical dispersion of a large number of OLTs, as well as the problem that the user's service quality is difficult to guarantee due to the low utilization of network resource. A programmable, dynamic, unified centralized control architecture is urgently needed. The software defined network (SDN) is emerging as a promising centralized control architecture [1], [2], and has been widely applied and developed in the field of optical access networks. Similar to the development trajectory of traditional networks, the development of SDN can not avoid security issues [3]. In the SDN optical network, the information interaction may occur between any two communication nodes, and there are constantly new ONUs to join and delete, so communication between nodes is uncertain and is not suitable for pre-establishing security associations [4]. As the first line of defense for security protection, identity authentication technology can effectively identify the true identity of communication participants, and then provide a basis for subsequent determination of user rights and service scope, which is an important means to achieve confidentiality and integrity [5]. Therefore, it is necessary to study a secure and efficient authentication scheme between communication nodes [6].

Secure identity authentication between communication nodes is to verify the legality of the identity of the two parties. Only the legal nodes can establish a secure connection, and then request services and meet the requirements, so as to prevent illegal nodes from maliciously using network resources. This technology has attracted the research of a large number of scholars and institutions, and a lot of research results have emerged. He *et al.* [7] proposed a secure authentication scheme that does not require authentication of public keys. Potthast *et al.* [8] proposed a two-factor authentication scheme based on Web authentication architecture.

The associate editor coordinating the review of this manuscript and approving it for publication was Zijian Zhang.

He *et al.* [9] proposed a distributed authentication protocol and key establishment scheme to provide application-level end-to-end security. Yang Bo *et al.* [10] proposed an improved certificateless two-party authentication key agreement protocol. Gao *et al.* [11] designed a signature scheme combining node certificate and identity. Jiang *et al.* [12] proposed an improved 802.1x two-way authentication scheme based on public key cryptosystem and realized encryption of sensitive domains. At the same time, Open Source Foundation (ONF), International Telecommunication Union (ITU) and China Telecom Standardization Association and other standardization organizations, as well as open source organizations such as OpenDayLight and OPNFV are also actively carrying out research work in the field of SDN security, but there is still no clear industry standard on SDN security has been officially released [13].

A. OUR CONTRIBUTION

Based on the existing research, we propose a lightweight two-way authentication scheme LTWA based on SDOAN. Through the identity authentication of the communication node, the identity legitimacy is ensured and the two parties can securely communicate, and three security services of integrity protection, confidentiality protection and certifiable protection can be provided. The main contributions of this paper are as follows:

1) This paper proposes a lightweight security identity authentication scheme based on software-defined optical access network, and designs the functional model of the controller and OLT.
2) The proposed scheme introduces the CGA algorithm and the HGA algorithm without third party participation, so as to complete the first authentication binding and the non-first authentication binding between the communication nodes respectively.
3) This paper designs a general metric model to evaluate the overall metrics of the scheme. Different users can increase, delete and change the measurement factors according to their actual application requirements, and get a more appropriate metric.

B. ORGANIZATION

The remainder of this paper is organized as follows. In Section II, we analyze the communication interaction process based on SDOAN, including security threats. The overall design of the security authentication scheme is given in Section III. The security analysis and the formulated measured design are presented in Section IV. Section V is the experimental simulation and results of the scheme. Section VI concludes the paper.

II. COMMUNICATION INTERACTION AND RISK ANALYSIS FOR SDOAN

A. COMMUNICATION INTERACTION BASED ON SDOAN

When the switch and controller need to connect, the connection can be initiated by the controller or by the switch. First,

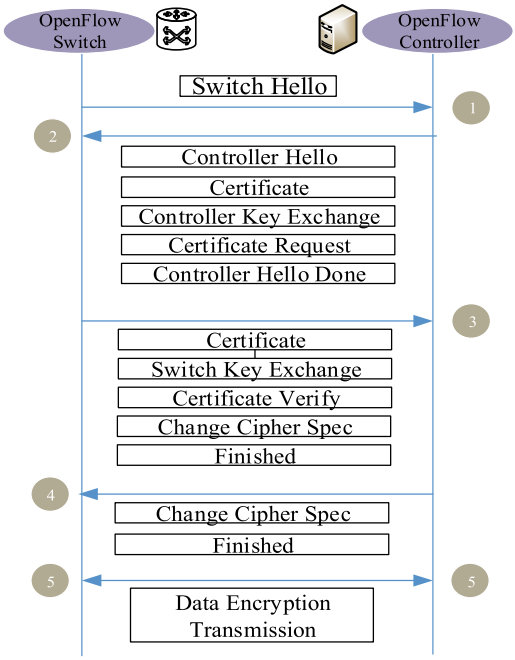


FIGURE 1. Switch-controller communication based on SSL/TLS.

the controller and the switch send Hello messages to each other. The Hello message only contains the OpenFlow Header. The version field in the header is the highest version of the OpenFlow protocol supported by the sender, and the two parties select the lowest version of the protocol in the Hello message as the communication protocol [14]. Assuming that one party does not support the OpenFlow protocol version, it sends an Error message and then disconnects. Otherwise, an OpenFlow connection is established. Then by establishing an SSL/TLS [15] secure connection to complete the identity authentication. The basic process is shown in the Fig. 1.

When the switch starts, it first tries to connect to the controller port specified by the user, and both parties authenticate each other by exchanging digital certificates. At the same time, each OpenFlow switch needs to be configured with at least two certificates, one is used to authenticate the legitimacy of the controller, and one is used to prove its legitimacy to the controller.

B. SECURITY THREATS DURING COMMUNICATION INTERACTION

Due to the complexity of the SSL/TLS protocol authentication process and the vulnerability of the SSL/TLS protocol itself, the OpenFlow protocol sets SSL/TLS as an option after the OpenFlow protocol version 1.3, the control channel is allowed to communicate without taking any security measures, making the SDOAN very vulnerable to eavesdropping, message tampering or other attacks on the OpenFlow channel [16]. The specific threats are as follows:

1) Eavesdropping attack: When the control plane performs OpenFlow protocol interaction, the attacker may intercept the protocol information and crack the

content of the message as the first step to launch a security attack.

2) Blocking attack: When an illegal network element in SDON generates a large number of optical connection requests, it triggers a large amount of control and interaction information, causing the optical network load to increase rapidly and the blocking rate to deteriorate.
3) Message tampering: A network attacker uses the intercepted protocol message to forge, destroying the establishment of a service connection, causing a normal optical connection failure.
4) Replay attack: The network attacker copies the intercepted protocol message and transmits the message repeatedly, which destroys the normal protocol interaction process.
5) Traffic analysis: The attacker may obtain the mode of protocol interaction and the process of message interaction through traffic analysis of message interaction.

In summary, the optical access network based on SDN faces many security threats, and the identity defense technology as the first line of defense for security interaction will provide important security guarantees for optical networks with multiple services.

III. LIGHTWEIGHT TWO-WAY AUTHENTICATION SCHEME

At present, the identity authentication method for the communication node can be classified according to the participation of the third party. The authentication scheme with third-party participation means that the authentication server needs to provide support during the authentication process. The participation of the server makes the security of these schemes better guaranteed, but there are shortcomings such as complexity and time consuming. The authentication scheme without third party participation means that no authentication server provides support during the authentication process. The algorithm or scheme itself provides authentication services, requiring both parties to have strong authentication computing capabilities. Compared with the former, the latter has the advantages of simple algorithm and high efficiency [17]. Aiming at the problems of the secure communication scheme in the existing SDOAN, the paper proposes a lightweight two-way identity authentication scheme. The scheme used the CGA algorithm [18] and the improved HGA algorithm [19] without third party participation to complete the first and non-first authentication binding between communication nodes respectively.

A. PRELIMINARY WORK OF THE SCHEME

1) PRINCIPLES OF THE SCHEME DESIGN

The design of the identity authentication scheme needs to be combined with the specific application environment and a reasonable authentication interaction process is established [20]. Based on the communication characteristics of software-defined optical networks, the overall flow chart

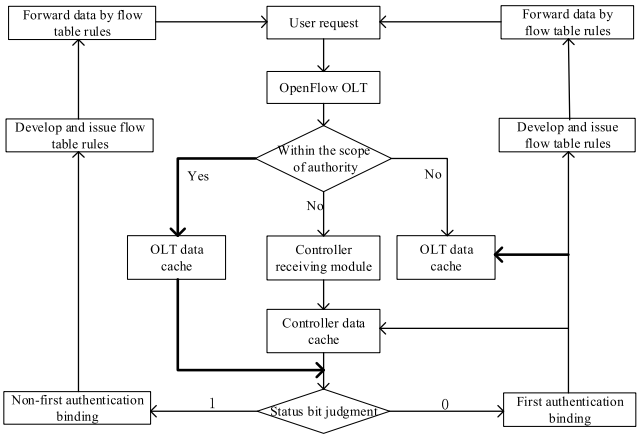


FIGURE 2. The overall flow chart design of the scheme.

design of the scheme is shown in the Fig. 2 and follows the following principles. Firstly, in order to achieve identity authentication between participants and establish a secure encryption key, it is necessary to maintain a certain complexity in designing the scheme; Secondly, considering the application requirements in the actual environment, the implementation efficiency and computational cost of the scheme need to be included in the criteria for measuring the performance of the scheme.

In addition, the certification scheme needs to meet the definition of lightweight, mainly including the following aspects.

1) During the equipment authentication process, minimize or not use third-party services to reduce the risk of uncertainty caused by third-party.
2) Under the condition that the computing power of the device is limited, the algorithm is required to be simple, the execution speed is fast, the computing resource consumption is small.
3) The device authentication process is as simple as possible, and the number of interactions is as small as possible.
4) The data in the device authentication process should be kept confidential and complete.
5) Any party involved in the communication cannot pre-set the encryption key and should make an equal contribution to the generation of the encryption key [21].

2) FUNCTIONAL MODULE DESIGN OF THE CONTROLLER AND THE OLT

In SDOAN, the controller and OLT are two core parts. The controller performs unified control for the underlying forwarding device through the southbound interface, and provides network resource calls to the upper layer service application through the northbound interface [22]. The control functions of the OLT are removed and the entire architecture is controlled by the controller. The OLT only performs the corresponding rights and operations according to the controller's instructions and policies through the OpenFlow intelligent agent, and reports the requests that cannot be processed

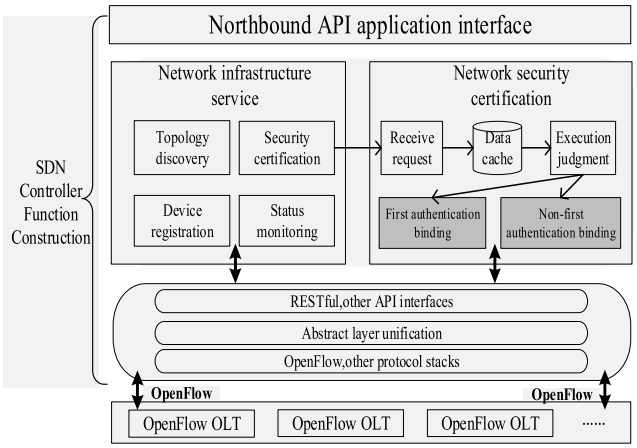


FIGURE 3. Function construction of SDN controller.

to the controller for processing. So the availability, reliability, and efficiency of the controller and the OLT are the premise and basis for the normal operation of the SDOAN architecture. In this paper, because the security scheme of identity authentication is introduced in the software-defined optical access network, the controller and OLT functional modules need to be designed and divided to meet the actual application requirements. The functional modules of the controller and OLT are designed as shown in Figs 3–4.

In Fig. 3, the underlying OpenFlow OLT sends the received user request to the controller through the protocol stack. The role of the protocol stack is to establish a secure channel and process the message. Then the abstraction layer normalization module of the controller converts the processed message into an advanced data model, describing the resources and strategies in an easily identifiable form of information. The converted request is provided to the network basic service function module through API interfaces such as RESTful and RPC. The network basic service function module mainly includes topology discovery, device registration, status monitoring, and security authentication. After receiving the user request, the controller sends it to the security authentication function module. The security detection function module mainly includes request reception, data cache, first authentication binding and non-first authentication binding. After the authentication binding is successful, the service is provided to the user through the northbound API application interface. The design of this controller provides functional module support for the enhancement of security protection for the software-defined optical network.

In Fig. 4, it can be seen that the software part of the OLT mainly includes three main functional modules: OpenFlow agent, Network basic service and PON. The OpenFlow agent module is mainly responsible for enabling the OLT to have the ability to interact with the SDN controller, while providing conditions for the OLT to exercise the rights and policies of the controller. The network basic service function module mainly includes the bandwidth allocation, the configuration management, the performance management, and the alarm

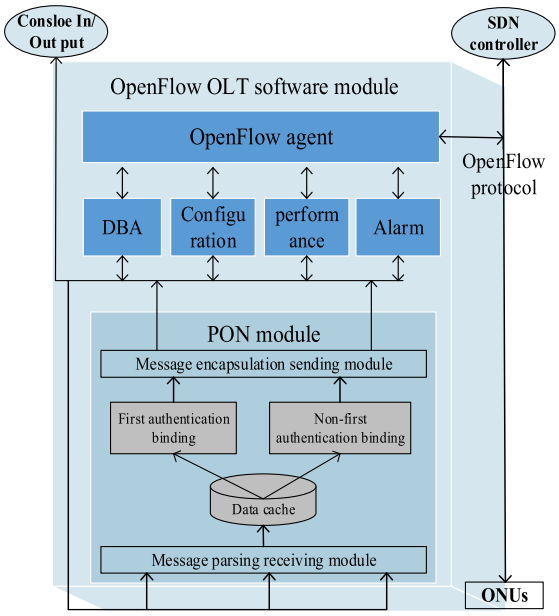


FIGURE 4. Function construction of OpenFlow OLT.

TABLE 1. The complete data structure of CGA.

Modifier Value (16B)	Subnet Prefix (8B)	Collision Value (1B)	Public Key (Variable Length)	Extended Domain (Option,Variable Length)

management [23]. The PON module mainly includes the message parsing receiving module, the message encapsulating sending module, and the security authentication binding module. The user request information is parsed and sent to the security authentication binding module. First, the security test is performed. After the test is passed, it is judged whether the first authentication binding or the non-first authentication binding is performed according to the status value, and then the subsequent corresponding interaction process is completed.

3) CGA PARAMETER SETTING AND KEY ALGORITHM SELECTION

The process of generating a new CGA address takes three input values: a 64-bit subnet prefix, the public key of the address owner, and the security parameter Sec, which is an unsigned 3-bit integer. The result is a new CGA address and the associated parameters. The complete data structure of the CGA consists of the modifier value, the subnet prefix, the collision value, the public key, and the extended domain by a certain logical relationship. Its data structure is shown in the Table 1.

The cost of generating a new CGA address depends largely on the length of the secret key used by the hash value. The length of the key determines the security level of the algorithm and the generation time of the hash value. It also indirectly determines the efficiency of the entire scheme. At present, most researches use RSA [24] as the default generation algorithm of the Public Key parameter in the CGA

algorithm, and the two are bound as RSA-CGA. One of the characteristics of the RSA algorithm is that the mathematical principle is simple and easy to implement in engineering applications, but its unit security level is relatively low, and the difficulty of deciphering or solving is only sub-exponential. The mathematical theory of ECC algorithm is relatively complicated, but its unit security level is relatively high. The difficulty of deciphering or solving is basically exponential, which makes the unit security streng th of ECC algorithm higher than RSA algorithm. In other words, to achieve the same security level, the key length required for the ECC algorithm is much lower than that of the RSA algorithm, which effectively solves the efficiency problem caused by the need to increase the key length in order to improve the security level. Therefore, we will replace the RSA algorithm with the ECC algorithm with more obvious advantages, and bind it to the CGA algorithm as ECC-CGA.

B. OVERALL AUTHENTICATION PROCESS OF THE SCHEME

1) THE FIRST AUTHENTICATION BINDING

The first authentication binding means that there is no communication between the optical switching node and the controller in the past time t, and no information about the other party is stored between them. The first authentication binding should be performed as follows.

Step1: When the optical switching node receives the service request from the user terminal, it will obtain a new address bound to the public key through the CGA algorithm. Then the optical switching node sents these contents of the new address, random number, timestamp, partial parameter information encrypted with the controller public key as Ecp(parameters1) and the status bits to the controller as parameters of the Packet-In message. At the same time, the relevant parameters2 are substituted into the Eq.1 to generate a session key (S_K) for subsequent data encryption.

$$S_K = First(128, parameters2). \tag{1}$$

Step2: After receiving the Packet-In message, the controller first initiates the attack detection. If the corresponding security attack is detected, the controller determines that the optical switch node has a security threat, cancels the service connection request, and records the security attack. If the security threat level is higher than the threshold set in advance, the controller notifies the corresponding module to update the relevant key. If the test passes, the controller first gets the CGA data structure and the parameters1 by decrypting the message with its own private key to verify whether the source address is legal. The specific verification steps are as follows:

1) Check that the ''g'' and ''u'' bits in the interface identifier are both zero. If either bit is non-zero, the CGA verification fails.
2) Decode the DER encoded Parameters data and judge. Check if the subnetPrefix data value is equal to the subnet prefix of the address (the leftmost 64 bits). Check if the collisionCount value is 0, 1 or 2. If the CGA parameter cannot be decoded, or the subnetPrefix value does not match the address, or the collisionCount value is out of range, the CGA verification fails.
3) Execute the hash algorithm on the DER-encoded CGA-Parameters data value. Take the leftmost 64 bits of the hash value. The result is Hash3.
4) Compare Hash3 to the interface identifier of the address (the right most 64 bits). Ignore the differences of the ''g'' bit, ''u'' bit and the leftmost three bits. If the 64-bit values are different (except for the five ignored bits), the CGA verification fails. If they are the same, continue with the step5.
5) Read the security parameter Sec from the leftmost three bits of the 64-bit interface identifier of the address. Set the subnetPrefix data value in the encoded CGAParameters data item to 8 zero octets, and the collisionCount data value to 0.
6) Execute the hash algorithm on the new DER-encoded CGAParameters data value. Take the 112 leftmost bits of the hash value. The result is Hash4.
7) Multiply the leftmost 16 bits of Hash4 with the Sec bit and compare the result with zero. If either bit is non-zero, the CGA verification fails. Otherwise, the verification is successful, the verifier knows that the Publickey field in the CGAParameters data value is the trusted public key of the address owner.

If it is legal, the parameters1 are re-encrypted with the public key of the optical switching node. Then as a parameter of the return information is encapsulated in the flow table entry of the Modify message along with the routing information parameter calculated by the controller. At the same time, all the parameter information is stored, and the parameters2 are also substituted into the Eq.1 to generate a S_K for subsequent data encryption.

Step3: After receiving the Modify message from the controller, the optical switching node also first performs attack detection. If the detection passes, the optical switching node decrypts the message with its own private key, and determines whether the obtained information is the same as the parameters1 sent in step 1, thereby verifying the identity of the controller. Then the optical switching node digitally signs the fixed value object such as the wavelength label, encrypts the parameters1 with the Publickey, and encapsulates them in the Reply message to the controller.

Step4: After receiving the Reply message, the controller verifies that the received parameters1 are the same as the previous ones received by the Publickey. If the parameters1 are the same, the controller confirms the identity of the optical switching node, establishes a data cache in itself. Then the controller sends an acknowledgment message to the optical switching node.

2) THE NON-FIRST AUTHENTICATION BINDING

Fig. 5 shows the process of the non-first authentication binding. The non-first-time authentication binding means that

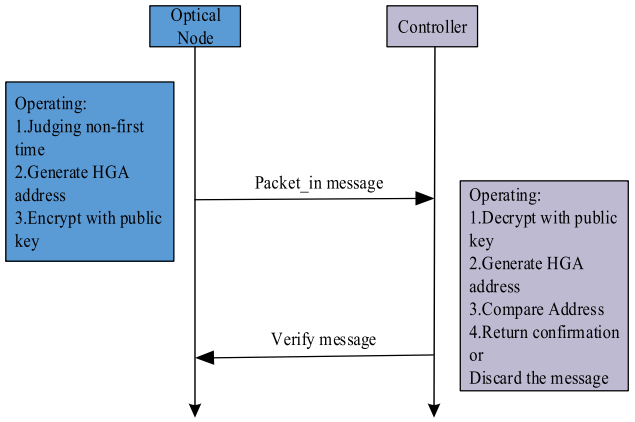


FIGURE 5. The process of the non-first authentication binding.

the optical switching node has communicated with the controller in the past time t, and has the shared key under the first authentication binding. When the location of the optical switching node changes or the authentication binding expires, the authentication binding needs to be performed again. The shared key saved during the first authentication binding process plays a key role, and it can still serve as information to prove its identity to the other party.

Considering the large computational cost of the CGA algorithm in the address generation and verification process, we propose the HGA algorithm to replace the CGA algorithm in the non-first authentication binding process.

Algorithm 1 Hash Generated Address

```
begin /*Begin of process*/
1 Input: (Public Key, Random Number, Link_Prefix)
2 {
3  Hash = MD5 (PK | RN | L_P)
4  User_ID = First(64, Hash)&0xfcff ffff ffff ffff
5 }
6 Output:A address generated by the HGA
7 {
8  HGA = Link_Prefix | User_ID
9  if (DAD(HGA)== pass)
10 {
11   goto 21
12 }
13 else
14 {
15   choose a new Random Number
16   goto 3
17 }
18 }
19 Verification: Address consistency
20 {
21 Send E(related parameters, HGA) to controller
22 D(related parameters, HGA) by controller
23 Controller recalculates the address
24 if (the calculated address == the packet address)
25 {
26   Verification success
27   Identity is legal
28 }
29 else
30 {
31   Verification failed
32   Discard the message
33 }
34 }
end /*End of process*/
```

IV. SECURITY ANALYSIS AND FORMULATED MEASURED DESIGN OF THE SCHEME

A. SECURITY ANALYSIS OF THE SCHEME

For the proposed security scheme, we mainly perform security analysis from five aspects: integrity protection, internal attack protection, replay attack protection, redirection attack and denial of service attack.

1) Integrity protection: By digitally signing and verifying the message digest of the fixed object in the message, detecting tampering attacks from external and internal messages to achieve integrity protection of signaling messages.
2) Internal attack protection: The important variable objects adopt the feedback comparison method to prevent the QoS parameters from being maliciously falsified by the illegal nodes to ensure the consistency between the actual optical connection and the service request.
3) Replay attack protection: prevent the malicious node from replaying the message by setting the serial number and the timestamp in the packet message.
4) Redirection attack protection: After the packet arrives, the identity authentication is performed, and the illegal data packet is directly discarded. Even if the data packet is redirected, because the attacker does not have the corresponding key and cannot decrypt it to ensure the security of the data packet.
5) Denial of service attack: When an attacker sends a large number of binding application packets, since the data packet needs to be encrypted and decrypted with the shared key, the invalid data packet will be blocked and discarded to prevent the denial of service attack.

It can be seen from the above analysis that the scheme is reliable in terms of security. In addition to the above security protection capabilities, the LTWA scheme maintains overall consistency with the original OpenFlow protocol and information interaction process, so it does not require additional signaling overhead and conforms to the definition of lightweight features.

B. FORMULATED MEASURED DESIGN OF THE SCHEME

In order to have a comprehensive evaluation of the scheme, we design a general metric model. The model assumes that

the entire network has n communication nodes, and its set is {N1, N2, N3,,, Nn}. N_o is the source node, N_d is the destination node. All nodes meet the requirements for integrity, confidentiality, availability required during the communication interaction [25]. The model takes the safety satisfaction, the blocking rate satisfaction and the delay satisfaction as the measurement factors of the scheme. Different users can increase, delete and change the measurement factors according to their actual application requirements, and then get a more appropriate metric model.

The secure connection (SC) between node N_o and node N_d is denoted as SC(N_o, N_d). The value of the secure connection metric that satisfies the relevant factors between nodes N_o and N_d is denoted as $D_{SC(N_o,N_d,factors)}$. The metric calculation is as shown in Eq. 2.

$$D_{SC_{(N_o,N_d,V_S,V_B,V_D)}} = w_1 \cdot \sum_{o}^{d} \frac{1}{V_S} + w_2 \cdot \sum_{o}^{d} \frac{1}{V_B} + w_3 \cdot \sum_{o}^{d} \frac{1}{V_D} \quad (2)$$

In this equation, V_S is expressed as safety satisfaction, V_B is expressed as blocking rate satisfaction (blocking rate is P_b, so $V_B = 1 - P_b$), and V_D is expressed as delay satisfaction; w_1, w_2 and w_3 are the weights corresponding to the above three metric factors, and satisfy the constraint condition of $w_1 + w_2 + w_3 = 1$.

V. EXPERIMENTAL SIMULATION AND RESULT

In order to carry out the experimental evaluation, we first implement the CGA algorithm through the Java language, and compare the original combined RSA algorithm with the ECC algorithm we used. By setting the relevant parameters, we compare the generation time of the hash value in the first authentication binding process, and calculate the average value under different security level. The experimental comparison results are shown in Fig. 6. Moreover, we use OMNeT ++ network simulation software to build a typical software-defined optical network application scenario [26]. From the two aspects of blocking rate and average authentication binding time, we compare the LTWA authentication scheme, SSL/TLS authentication scheme and hash node authentication scheme (HNA) [27] under different constraints. The experimental scenario consists of one OpenFlow controller, 6 OLT nodes, and 96 ONU nodes. The uplink and downlink rates are set to 10 Gbps, the distance from the controller to the OLT is set to 50 km, the distance from the OLT to the ONU is set to 20 km. The comparison results are shown in Figs. 7-8.

Fig. 6 shows the comparison results of the generate hash time under different security levels. As the security level increases, the key length of both the RSA and the ECC increases, but the RSA key length increases quickly, and the ECC key length increases slowly. Moreover, when the security level is the same, for example, the key security level 1024 bit length of RSA is equivalent to the key security level 163 bit length of ECC. Since the ECC algorithm has a shorter key length, the hash value time for generating the CGA is much smaller than the RSA algorithm.

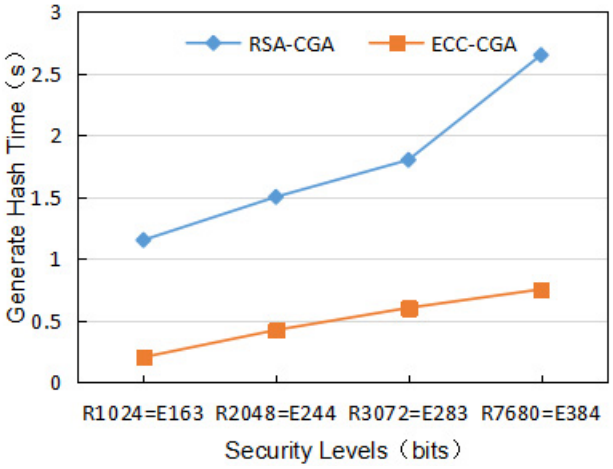


FIGURE 6. Comparison of hash generation time under different security levels.

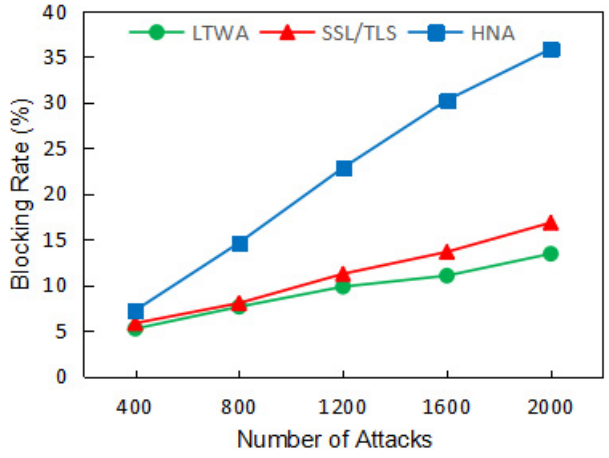


FIGURE 7. Comparison of blocking rates under different attack times.

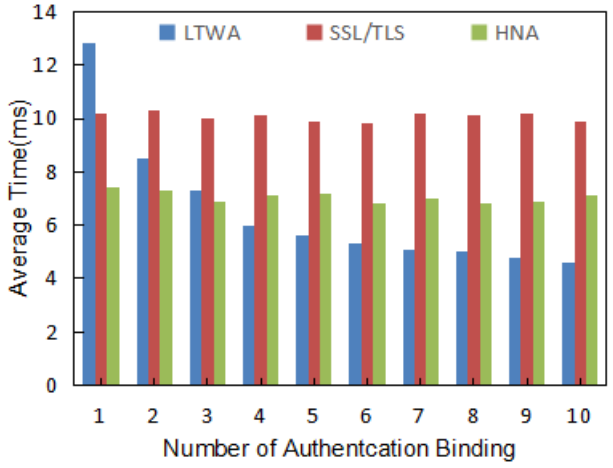


FIGURE 8. Average time spent under different authentication binding times.

Fig. 7 shows the comparison results of the blocking rate under different attack times. It can be seen that as the number of attacks increases, the blocking rate increases, but the

LTWA scheme is superior to the other two schemes and is significantly better than the traditional authentication scheme HNA. Because the traditional authentication scheme HNA only implements one-way identity authentication through the hash algorithm, it is more vulnerable to the threat of security attacks. These attacks lead to confusion in signaling processing and illegal occupation of resources, which causes the failure of the service establishment and leads to higher blocking rate.

Fig. 8 shows the average time spent under different authentication binding times. It can be seen that the LTWA scheme only takes more time in the first authentication binding, because the first process uses an asymmetric encryption algorithm and involves key negotiation, so the message interaction is more. As the number of authentication bindings increases, the proportion of non-first authentication bindings increases. However, the non-first authentication binding process uses the symmetric encryption algorithm and the HGA algorithm, which eliminates excessive message interaction and simplifies the authentication binding process. Therefore, the average time consumption of the LTWA scheme gradually decreases as the number of interactions increases until it is close to the time of a single non-first authentication binding, which improves the communication efficiency and reduces the average cost.

VI. CONCLUSION

For the problem that high security and low overhead are difficult to balance in the communication process of OpenFlow optical access network, this paper proposes a lightweight two-way identity authentication scheme between communication nodes. In the case that the communication parties have no shared key, the scheme uses the asymmetric encryption algorithm and the CGA algorithm to complete the first authentication binding and negotiate the public key. Moreover, the scheme uses the symmetric encryption algorithm and the HGA algorithm to complete the non-first authentication binding in a relatively simplified process and protect the security of the message. Finally, the simulation results show that the scheme can meet the high security interaction requirements with low resource overhead in the OpenFlow optical access network and meet the requirements of lightweight definition.

REFERENCES

[1] H. Yang, J. Zhang, Y. Zhao, J. Wu, Y. Ji, Y. Lin, J. Han, and Y. Lee, "Experimental demonstration of remote unified control for OpenFlow-based software-defined optical access networks," *Photonic Netw. Commun.*, vol. 31, no. 3, pp. 568–577, 2016.

[2] F. Paolucci, F. Civerchia, A. Sgambelluri, A. Giorgetti, F. Cugini, and P. Castoldi, "P4 edge node enabling stateful traffic engineering and cyber security," *J. Opt. Commun. Netw.*, vol. 11, no. 1, pp. A84–A95, 2019.

[3] A. Akhunzada, E. Ahmed, A. Gani, M. K. Khan, M. Imran, and S. Guizani, "Securing software defined networks: Taxonomy, requirements, and open issues," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 36–44, Apr. 2015.

[4] H. Yang, W. Bai, A. Yu, and J. Zhang, "Performance evaluation of software-defined clustered-optical access networking for ubiquitous data center optical interconnection," *Photonic Netw. Commun.*, vol. 34, no. 1, pp. 1–12, 2017.

[5] R. Khondoker, P. Larbig, D. Senf, K. Bayarou, and N. Gruschka, "AutoSecSDNDemo: Demonstration of automated end-to-end security in software-defined networks," in *Proc. IEEE NetSoft Conf. Workshops*, Jun. 2016, pp. 347–348.

[6] M. Chen, Y. Qian, S. Mao, W. Tang, and X. Yang, "Software-defined mobile networks security," *Mobile Netw. Appl.*, vol. 21, no. 5, pp. 729–743, 2016.

[7] D. He, S. Padhye, and J. Chen, "An efficient certificateless two-party authenticated key agreement protocol," *Comput. Math. Appl.*, vol. 64, no. 6, pp. 1914–1926, 2012.

[8] M. Potthast, C. Forler, E. List, and S. Lucks, "PASSPHONE: Outsourcing phone-based Web authentication while protecting user privacy," in *Proc. Nordic Conf. Secure IT Syst.*, 2016, pp. 235–255.

[9] D. He, S. Zeadally, N. Kumar, and W. Wu, "Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2052–2064, Sep. 2016.

[10] Y. W. Zhou, B. Yang, and W. Z. Zhang, "An improved two-party authenticated certificateless key agreement protocol," *Chin. J. Comput.*, vol. 40, no. 5, pp. 1181–1191, 2017.

[11] T. H. Gao, N. Guo, and Z. L. Zhu, "Access authentication for HMIPv 6 with node certificate and identity-based hybrid scheme," *J. Softw.*, vol. 23, no. 9, pp. 2465–2480, 2012.

[12] H. Jiang, L. Q. Zhang, and L. L. Ruan, "Study on public key cryptography-based 802.1x bidirectional authentication," *Comput. Appl. Softw.*, vol. 33, no. 2, pp. 290–293, 2016.

[13] M. M. Wang, J. W. Liu, J. Chen, J. Mao, and K. F. Mao, "Software defined networking: Security model, threats and mechanism," *J. Softw.*, vol. 27, no. 4, pp. 969–992, 2016.

[14] Y. H. Fu, J. Bi, K. Y. Zhang, and J. P. Wu, "Scalability of software defined network," *J. Commun.*, vol. 38, no. 7, pp. 141–154, 2017.

[15] A. Aguado, V. Lopez, J. Martinez-Mateo, T. Szyrkowiec, A. Autenrieth, M. Peev, D. Lopez, and V. Martin, "Hybrid conventional and quantum security for software defined and virtualized networks," *J. Opt. Commun. Netw.*, vol. 9, no. 10, pp. 819–825, 2017.

[16] J. Benabbou, K. Elbaamrani, N. Idboufker, and R. Elassali, "Software-defined networks, security aspects analysis," in *Proc. 11th Int. Conf. Inf. Assurance Secur.*, Dec. 2015, pp. 79–84.

[17] J. Sayid, I. Sayid, and J. Kar, "Certificateless public key cryptography: A research survey," *Int. J. Secur. Appl.*, vol. 10, no. 7, pp. 103–118, 2016.

[18] T. Aura, "Cryptographically generated addresses (CGA)," in *Proc. Int. Conf. Inf. Secur.*, 2003, pp. 29–43.

[19] T. Rajendran and K. V. Sreenaath, "Hash optimization for cryptographically generated address," in *Proc. 3rd Int. Conf. Commun. Syst. Softw. Middleware Workshops*, Jan. 2008, pp. 365–369.

[20] Z. S. Eidgahi and V. Rafe, "Security analysis of network protocols through model checking: A case study on mobile IPv6," *Secur. Commun. Netw.*, vol. 9, no. 10, pp. 1072–1084, 2016.

[21] J. Cui, Y. Zhang, Z. Wang, and J. Liu, "Light-weight object detection networks for embedded platform," *Acta Optica Sinica*, vol. 39, no. 4, 2019, Art. no. 0415006.

[22] S. J. Zhang, J. L. Lan, Y. X. Hu, and Y. M. Jiang, "Survey on scalability of control plane in software-defined networking," *J. Softw.*, vol. 29, no. 1, pp. 160–175, 2018.

[23] R. Trivisonno, R. Guerzoni, I. Vaishnavi, and D. Soldani, "SDN-based 5G mobile networks: Architecture, functions, procedures and backward compatibility," *Trans. Emerg. Telecommun. Technol.*, vol. 26, no. 1, pp. 82–92, Jan. 2015.

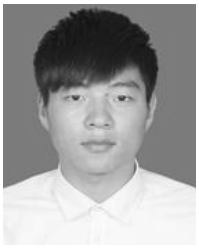
[24] X. L. Li and W. J. Ai, "Research on a security binding mechanism based on communication node identity authentication," *Comput. Appl. Softw.*, vol. 32, no. 1, pp. 294–296, 2015.

[25] A. Lara and B. Ramamurthy, "OpenSec: Policy-based security using software-defined networking," *IEEE Trans. Netw. Service Manag.*, vol. 13, no. 1, pp. 30–42, Mar. 2016.

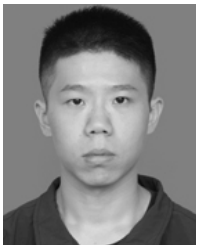
[26] S. Azodolmolky, M. N. Petersen, A. M. Fagertun, P. Wieder, S. R. Ruepp, and R. Yahyapour, "SONEP: A software-defined optical network emulation platform," in *Proc. Int. Conf. Opt. Netw. Design Modeling*, May 2014, pp. 216–221.

[27] Z. Q. Guo, Z. X. Wang, L. C. Zhang, and Y. Z. Kong, "An efficient and secure route optimisation scheme for mobile IPV6 based on hash generate address," *Comput. Appl. Softw.*, vol. 33, no. 6, pp. 105–109, 2016.

YONGLI TANG received the M.S. degree from Henan Polytechnic University, in 2005, and the Ph.D. degree from the Beijing University of Posts and Telecommunications, in 2008. He visited Dublin City University, Ireland, in 2013. He is currently a Professor with the School of Computer Science and Technology, Henan Polytechnic University. His research interests include modern cryptography, networks, and information security.



TAO LIU received the B.S. degree from Henan Polytechnic University, in 2016, where he is currently pursuing the M.S. degree. His research interests include software-defined networks, intelligent networks, and network security.



XU HE received the B.S. degree from Hebei Agricultural University, in 2016. He is currently pursuing the M.S. degree with Henan Polytechnic University. His research interests include modern cryptography and network security.

JINXIA YU received the M.S. degree from the Jiaozuo Institute of Technology, in 2003, and the Ph.D. degree from Central South University, in 2007. She is currently a Professor with the School of Computer Science and Technology, Henan Polytechnic University. She is mainly involved in artificial intelligence, pattern recognition, and network security.

PANKE QIN received the M.S. degree from the China University of Geosciences, in 2009, and the Ph.D. degree from the Beijing University of Posts and Telecommunications, in 2015. He is currently a Lecturer with the School of Computer Science and Technology, Henan Polytechnic University. His research interest includes software-defined optical networks and artificial intelligence.