一种基于 OpenFlow 光接入网的轻量级安全身份认证加密机制

汤永利[1]，刘涛[1]，李一鸣[2]，叶青[1]，秦攀科[1]*

[1]河南理工大学计算机科学与技术学院，河南 焦作 454000；

[2]上海大学通信与信息工程学院，上海 200444

摘要 为满足互联网多业务背景下各方对于安全性的更高要求，平衡因引入安全机制造成的高代价问题，通过分析软件定义光接入网(SDOAN)所面临的通信安全挑战，提出了一种基于加密生成地址(CGA)算法与哈希生成地址(HGA)算法相结合的轻量级安全身份认证加密机制(CH-CNA)。该机制遵循 OpenFlow 协议的信息交互方式，通过引入无第三方参与的 CGA 算法和 HGA 算法，以此分别完成通信节点之间的首次认证绑定和非首次认证绑定。在认证绑定过程中可有效防止攻击者伪造、篡改认证交互消息，从而建立起面向接入网的端到端可信连接。采用 OMNeT++网络仿真软件对提出的 CH-CNA 机制进行了测试，实验结果表明，该机制在保证通信节点之间安全性交互的同时，降低了平均计算开销和因恶意攻击引起的阻塞率，符合轻量级的定义要求。

关键词 光通信；协议；软件定义网络；认证；加密生成地址算法；哈希生成地址算法

中图分类号 TN929 **文献标识码** A **doi**：10.3788/AOS201939.0906002

Lightweight Secure Identity Authentication Encryption Mechanism Based on OpenFlow Optical Access Network

Tang Yongli[1], Liu Tao[1], Li Yiming[2], Ye Qing[1], Qin Panke[1]*

[1] *College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, Henan* 454000, *China*;

[2] *School of Communication and Information Engineering, Shanghai University, Shanghai* 200444, *China*

Abstract We propose a lightweight secure identity authentication encryption (CH-CNA) mechanism based on the cryptographically generated address (CGA) algorithm and the hash generated address (HGA) algorithm to satisfy the strict security requirements of all the parties in the internet multi-servicing context while reducing the cost that is typically associated with the introduction of security mechanisms. In particular, the proposed mechanism analyzes the communication security challenges faced by the software-defined optical access networks (SDOAN). The CH-CNA mechanism follows the information interaction method of the OpenFlow protocol, and the first and non-first authentication bindings are achieved among the communication nodes using the CGA and HGA algorithms without any third-party participation. During the authentication binding process, the attacker is prevented from forging or tampering with the authentication interaction messages, establishing an end-to-end trusted connection in the access network. The proposed CH-CNA mechanism is tested using the OMNeT++ network simulation software. The experimental results demonstrate that the proposed mechanism can reduce the average computational overhead and blocking rate because of malicious attacks and ensure secure interaction among the communication nodes, which conforms to the definition of lightweight.

Key words optical communication; protocol; software-defined network; authentication; cryptographically generated address algorithm; hash generated address algorithm

OCIS codes 060.2330; 060.4510; 060.4785

收稿日期：2019-03-27；**修回日期**：2019-04-16；**录用日期**：2019-05-05

基金项目：国家自然科学基金(61802117)、“十三五”国家密码发展基金(MMJJ20170122)、河南省科技厅项目(142300410147，182102310923)、河南省教育厅项目(18A413001，16A520013)、河南理工大学创新型科研团队(T2018-1)

* **E-mail**：qinpanke@hpu.edu.cn

1 引 言

随着网络用户数量的急剧增长，互联网业务朝着流量、种类等多维度方向迅猛发展。无论是运营商还是用户都迫切需要一种可编程的、动态的、统一的集中式控制架构，来解决因设备地理分散和数量庞大而导致的运维成本增加的问题，以及因不同用户的数据流量缺乏动态控制和智能调度而导致的网络资源利用率低下和用户需求难以保证的问题。在此情形下，OpenFlow 协议支持的软件定义网络(SDN)作为一种有前景的集中式控制体系架构应运而生[1-2]，并在光接入网领域得到了广泛的应用和发展，达到了较好的预期和成效，但与传统网络的发展轨迹类似，其发展仍旧避不开安全保障问题。若安全问题能得到很好的解决，将会有力地推动接入网等各项通信技术的快速发展[3]。

在软件定义光网络中，一个控制器控制多个光线路终端(OLT)，每个 OLT 又同时连接多个光网络单元(ONU)，整体的架构采用树形结构方式，因此安全问题容易以更加复杂和多样化的形式出现在架构的各个层次[4]。同时接入网中的信息交互可能发生在任意两个通信节点之间，并且不断有新的 ONU 的加入和删除，通信节点之间带有不确定性，不适合预先建立安全关联的方式。加之目前各方在接入网方面一味地追求效率，如何权衡安全机制与系统代价之间的关系就成为了各方目前面临并亟待解决的问题。在层次复杂、形式多样的网络安全防护中，将身份认证作为第一道防线，不但能够避免恶意节点入侵窃取网络资源，而且可以对每个合法使用网络资源的用户进行身份识别，是软件定义光接入网(SDOAN)通信安全和管理安全的重要保证[5]。因此，研究一种安全与高效兼顾的认证机制在控制器、OLT、ONU 之间建立安全防护就显得十分必要[6]。

众多的学者对通信节点间的安全身份认证技术进行了研究，并涌现了大量的研究成果：He 等[7]提出了一种不需要验证公钥(public key)的安全认证机制；Potthast 等[8]提出了一种基于 Web 认证架构的双因素身份认证方案；He 等[9]提出了一种分布式的认证协议和密钥建立方案，可提供应用级端至端的安全性；周彦伟等[10]提出了一种改进的无证书两方认证密钥协商协议；高天寒等[11]设计了一种节点证书与身份相结合的签名方案；蒋华等[12]提出了一种基于 public key 密码体制的 802.1x 双向认证改进方案，并实现了对敏感域的加密。与此同时，OpenDayLight、OPNFV 等开源组织、开放网络基金会(ONF)，以及中国电信标准化协会等标准化组织，也都陆续开展了 SDN 安全方面的研究工作，但至今仍没有明确的 SDN 安全方面的行业标准被正式发布[13]。对上述研究分析后，本文提出了一种基于 OpenFlow 光接入网的轻量级安全身份认证加密机制(CH-CNA)，通过对通信节点的身份认证来保证身份的合法性，并实现两者的安全通信，可提供完整性保护、机密性保护和可认证保护这三种安全性业务。

2 基于 OpenFlow 协议的信息交互风险分析

2.1 SDN 中的 OpenFlow 通信协议

控制层与设备层之间的 OpenFlow 协议是在 SDN 中最早被提出并且最具普遍适用性的协议，它凭借灵活的配置和规范的设定，早已成为 SDN 的标准通信协议[14]。基于 OpenFlow 光接入网的系统架构如图 1 所示，SDN 控制器作为架构的核心，通过 OpenFlow 协议对 PON(Passive Optical Network)接入网中的资源进行统一控制。设备之间的交互和每个扩展功能的实现都需遵循 OpenFlow 协议，OLT 和 ONU 都需要具有 OpenFlow 代理软件才能与控制器进行交互[15]。

2.2 基于 OpenFlow 的安全连接通信实例及风险分析

在交换机和控制器进行连接时，该连接可以由控制器发起，也可以由交换机发起。两者通过协商选取双方都支持的协议版本作为通信协议，成功建立 OpenFlow 连接。紧接着双方建立 SSL/TLS(Secure Sockets Layer/Transport Layer Security)[16]安全连接对消息进行加密和认证，基本过程如图 2 所示。

由图 2 可知，采用 SSL/TLS 协议的认证过程包含了通信双方之间的多次信息确认与交互，步骤十分繁琐。同时考虑到 SSL/TLS 协议本身的脆弱性，将其设置为可选项，即允许控制通道不采取任何安全措施进行通信，使得软件定义光网络极易遭到来自 OpenFlow 通道上的各项攻击[17]。

1) 窃听攻击：当控制平面进行 OpenFlow 协议交互时，攻击者可能截获这些协议信息，破解出消息的内容，作为发动安全攻击的第一步。

2) 阻塞攻击：软件定义光接入网中非法网元会生成大量的光连接请求，触发 OpenFlow 协议发起光连接的控制和交互信息，进而导致光网络负载剧

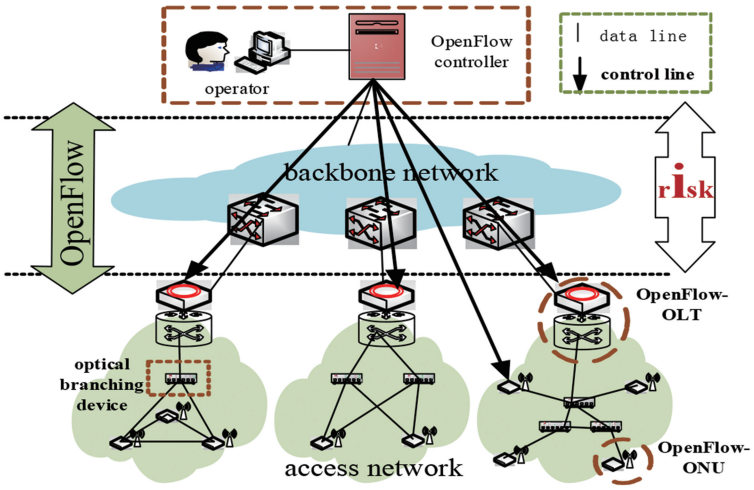

图 1　基于 OpenFlow 光接入网的系统架构

Fig. 1　System architecture based on OpenFlow optical access network

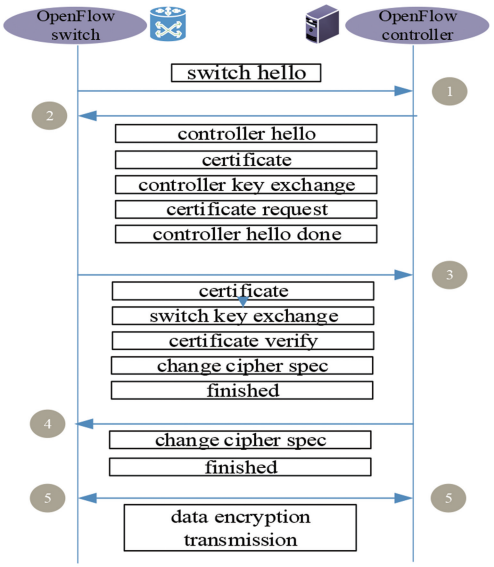

图 2　OpenFlow 交换机-控制器 SSL/TLS 通信实例

Fig. 2　OpenFlow switch-controller communication instance based on SSL/TLS protocol

增而阻塞率劣化。

3）消息篡改：网络攻击者利用截获到的协议消息进行伪造，破坏业务连接的建立，导致正常的光连接失败。

4）重放攻击：网络攻击者将截获到的协议消息进行复制，多次反复传送该消息，破坏正常的协议交互过程。

5）通信量分析：网络攻击者在一定的技术条件下有可能根据消息交互的流量，获取到协议交互的模式，包括光通信节点的标识以及协议消息的交互过程。

综上所述，基于 OpenFlow 的光接入网面临着众多的安全威胁，而身份认证技术作为安全交互的第一道防线将为软件定义光接入网提供重要的安全保证。

3　安全身份认证加密机制

目前对于结点的身份认证方法可以根据有无第三方的参与进行分类：有第三方参与的认证机制在认证过程中需要认证服务器提供支持，其在保证安全性的同时不免存在复杂、耗时等缺点；无第三方参与的认证机制在认证过程中仅靠算法或机制本身提供认证服务，不需要认证服务器的支持，具有算法简单、效率高等优势，但要求通信双方具备较强的认证计算能力[18]。针对现有软件定义光接入网中安全通信机制存在的问题，提出了一种轻量级安全身份认证加密机制。该机制摒弃了第三方的参与，利用攻击预防和入侵检测的原理[19]，对固定参数进行数字签名保护，并分别采用加密生成地址（CGA）[20]和改进的哈希生成地址（HGA）[21]两种生成地址算法完成通信节点间的首次和非首次认证绑定。

3.1　OpenFlow 协议扩展

OpenFlow 协议支持 controller-to-switch（控制器与网络设备间的交互）、symmetric（同步）、asynchronous（异步）这 3 种消息类型[22]。不同的消息类型所对应的报文信息是不同的，但总体格式却是一致的（由于实际需求某些内容会有所改变）。本研究因引入安全机制，需要对 OpenFlow 协议进行扩展，以 Flow-mod 消息为例，扩展形式如图 3 所示。

对于 OpenFlow 协议的扩展主要源于功能的需求和改进，所以扩展的内容主要包括指令集和 OpenFlow 端口这两个部分。当用户进行数据请求时，会触发用户身份认证的指令，进而根据指令集中

header			match		instruction			OpenFlow port		
type	length	xid	priority	counter	command	action	status	physics	logic	retention

图 3　以 Flow-mod 消息为例的 OpenFlow 协议扩展

Fig. 3　OpenFlow protocol extension using Flow-mod messages as example

的相应动作集和状态集进行一系列的后续操作。

有了上面的指令和动作后，还需要设置用于处理 OpenFlow 网络协议的网络接口，这些接口是设备之间信息交互的关键，将其设置为三种类型：物理端口、逻辑端口和保留端口。物理端口为硬件接口，逻辑端口为其他协议或模块的设置接口，保留端口是根据转发动作定义的接口，也是对协议再扩展的预留。

3.2　CGA 参数的设置及生成

CGA 的生成过程需要三个输入值：64 位子网前缀、地址所有者的 public key，以及三位整数的无符号安全参数 Sec。生成新 CGA 的成本很大程度上取决于哈希值生成时用到的 public key 的秘钥长度，而秘钥长度的大小决定了算法的安全强度以及哈希值生成时间的长短，也就间接地决定了整个方案的效率。目前，大多数研究将 RSA 算法作为 CGA 算法中 public key 这一参数的默认生成算法，将两者进行绑定称为 RSA-CGA 算法。RSA 算法的特点之一是数学原理简单，在工程应用中比较易于实现，但其单位安全强度相对较低，破译或求解难度仅为亚指数级。尽管 ECC（Elliptic Curve Cryptography）算法的数学理论相对复杂，但其单位安全强度相对较高，破译或求解难度基本上为指数级，也就意味着 ECC 算法的单位安全强度要高于 RSA 算法，即要达到同样的安全强度，ECC 算法所需的密钥长度远低于 RSA 算法，这就有效地解决了为提高安全强度必须增加密钥长度所带来的效率问题。因此，利用优势更加明显的 ECC 算法替换 RSA 算法，将两者进行绑定称为 ECC-CGA 算法。将设置好的相关参数信息与修饰符值、public key，以及扩展域等重新组合，便能够得到 CGA 完整的数据结构，如图 4 所示。

modifier (16 byte)	subnet prefix (8 byte)	collision (1 byte)	public key (variable length)	extended domain (option, variable length)

图 4　CGA 的完整数据结构

Fig. 4　Complete data structure of CGA

生成 CGA 和相关的参数设置应按照如下步骤进行，其地址生成流程如图 5 所示。

1）设置 CGA 数据结构。生成一个 128 位的随机数，并将其放入修正字段 modifier 中，将 public key 设置为地址所有者的 public key，将 subnet prefix 设置为 8 个 0 的八位字节，同时将 collision count 设置为零。

2）将参数字符串连接组成新的字符串 CGA parameters，进行 DER（Distinguished Encoding Rules）编码，执行哈希运算，并截取哈希值最左边的 112 位将其作为 hash 1。

3）截取 hash 1 最左边的 16 位与用户标识部分的前三位（即 Sec 位）相乘，若结果为 0（或 Sec 为 0），接着执行下面的步骤。否则，将修正字段值加 1 并返回步骤 2）。

4）将编码的 CGA parameters 数据项中的 8 个 8 位字节的 subnet prefix 设置为给定的子网前缀，并将 collision count 设为 0。

5）对新编码的 CGA parameters 数据值重新执行哈希算法。取哈希值的最左边 64 位，将其作为 hash 2。

6）通过将 hash 2 中的“u”和“g”位都设置为 0，并将地址最左边的三位设置为 Sec 位值，形成 CGA 的接口标识符。

7）通过结合给定的 64 位子网前缀与计算得到的 64 位接口标识符，便得到了一个新的 CGA 地址。

8）执行重复地址检测。当检测到地址冲突时，将当前数据结构中的 collision count 加 1，并返回步骤 5）。如若连续 3 次都发生地址冲突，则停止流程并报告错误。

当通信对端接收到发来的消息时，首先需要通

过消息中所包含的 CGA 数据结构以及参数信息对源地址的合法性进行验证，验证的整体流程如图 6 所示，具体的验证步骤因与 CGA 生成步骤有很多相似之处，在此不再赘述。

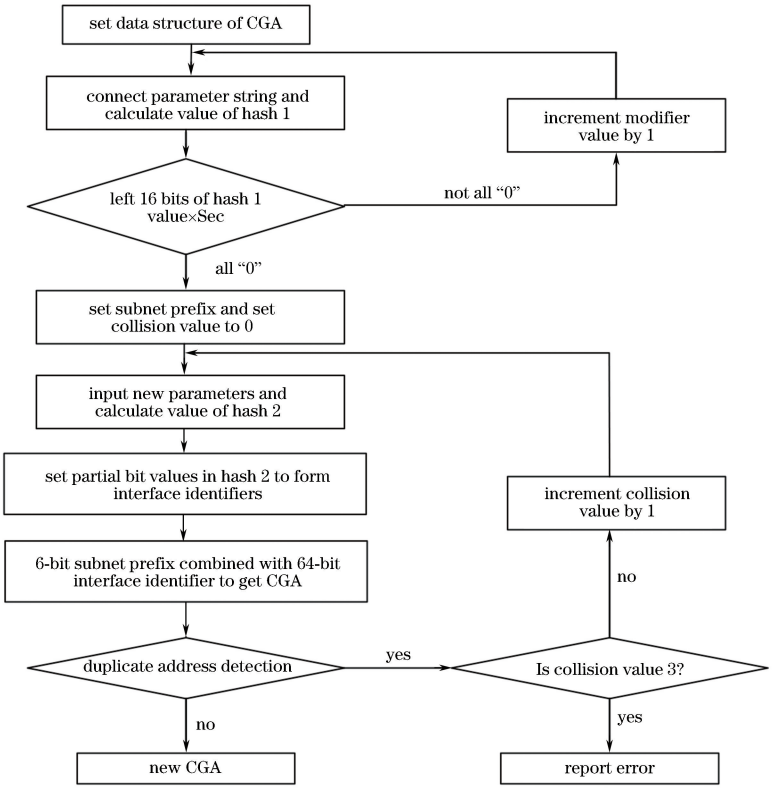

图 5　CGA 的生成流程

Fig. 5　Generation process of CGA

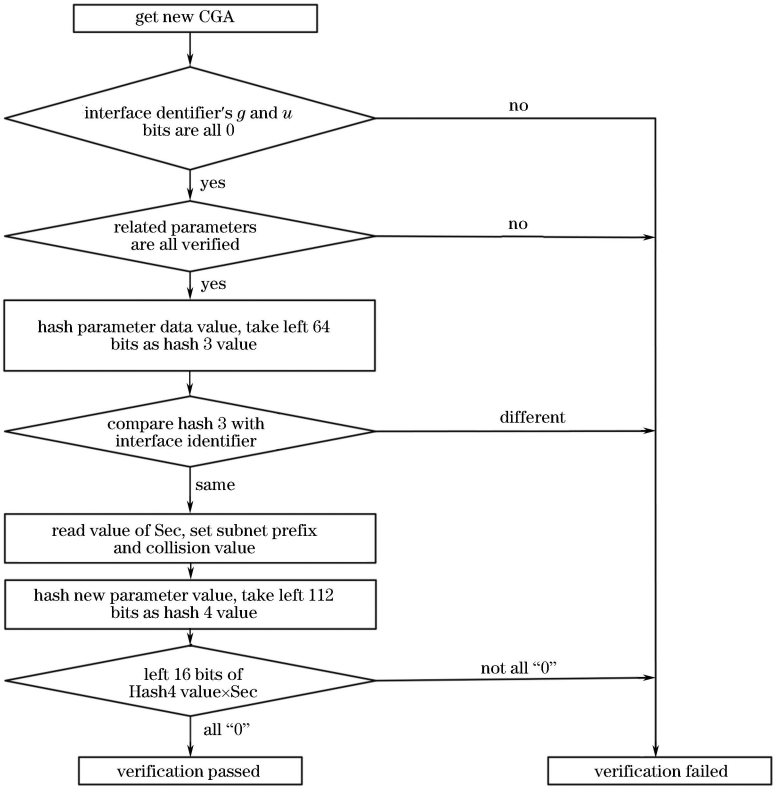

图 6　CGA 的验证流程

Fig. 6　Verification process of CGA

3.3　认证机制交互流程

3.3.1　通信节点间首次认证绑定

首次认证绑定是指在过去的时间 t 内，光交换节点与控制器之间无通信，且相互之间未存储任何关于对方的信息。首次认证绑定流程如图 7 所示。

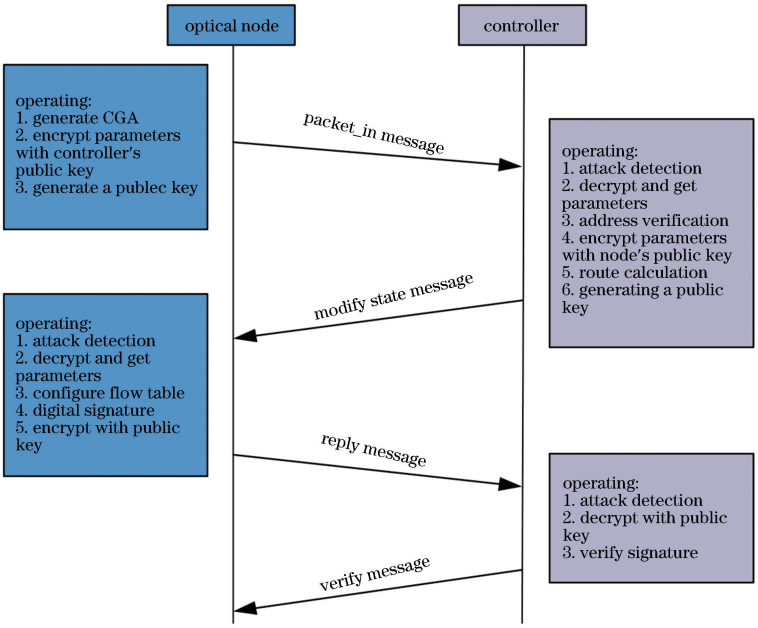

图 7　首次认证绑定流程

Fig. 7　Process of first authentication binding

Step 1：光交换节点收到用户请求时，将通过 CGA 算法得到一个与 public key 绑定的新地址，将其与随机数、时间戳、用控制器 public key 加密的部分参数信息 Ecp(P_1)，以及 status 状态位通过 packet-in 消息参数的形式一并传输给控制器。同时根据(1)式取相关参数 P_2 的前 128 位生成数据加密用的密钥，记为 K_{PK}[20]，其表达式如下

$$K_{PK}=\mathrm{First}(128,P_2)。\tag{1}$$

Step 2：控制器在接收到 packet-in 消息后，发起攻击检测，如果检测出相应的安全攻击，则取消该连接请求并记录。若检测通过，控制器首先用自身的私钥解密获得消息中载有的 CGA 数据结构和相关参数信息 P_1，以此来验证消息中的源地址是否合法。若合法，将参数信息 P_1 重新用对方的 public key 进行加密，将其与控制器计算出的路由信息作为参数一起封装在 modify-state 消息中传递。同时选择与 Step1 中相同的参数信息 P_2 利用(1)式生成密钥 K_{PK}，以备后续的数据加密使用。

Step 3：光交换节点接收到 modify-state 消息后，同样先进行攻击检测。若检测通过，则用自身私钥进行解密，如果与 Step 1 中发出的 P_1 相同，则控制器身份得以验证。同时对相关固定值对象进行数字签名，用 public key 加密 P_1 后封装在 reply 消息中发往控制器。

Step 4：控制器接收到 reply 消息后，通过 public key 验证收到的参数信息 P_1。若一致，控制器确认光交换节点的身份，并与之建立认证绑定关系。随后发送确认消息给光交换节点，完成首次认证绑定。

3.3.2　通信节点间非首次认证绑定

当光交换节点的位置发生变化或者是认证绑定的有效期结束时，需要重新进行认证绑定。此时，在首次认证绑定过程中保存下来的共享密钥就起到了关键性的作用，其依然能够作为向对方证明自身身份的信息。考虑到 CGA 算法在地址生成和验证过程中计算开销大的问题，对 HGA 算法进行替换，算法描述如图 8 所示。

1) 光交换节点首先需要判断与控制器协商的 K_{PK} 是否存在，若存在，则判定为非首次认证绑定。随后该节点使用改进的 HGA 算法生成新的地址，并通过非首次认证绑定的方式对控制器进行报文的传送。

2) 控制器收到报文后，根据 status 的值进行判断，0 表示首次建立认证绑定关系，1 表示非首次建立认证绑定关系。当 status 值为 1 的时候，控制器通过 public key 来解密信息，然后根据获取的参数，采用HGA算法重新计算出地址，并与报文中的地

```
begin /*Begin of process*/
 1  Input: (Public key, Random Number, Link_Prefix)
 2  {
 3    Hash = MD5 (Public key | Random Number | Link_Prefix)
 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 Epk(related parameters, HGA)  to controller
22    Dpk (related parameters, HGA) by controller
23    Controller recalculates the address
24    if (the calculated address == the address in the packet)
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*/
```

图 8　HGA 算法描述

Fig. 8　Description of HGA algorithm

址进行比较，如果两者相同，则验证通过，并返回确认信息，否则验证失败，丢弃报文。

3.4　机制的安全性分析及度量设计

对提出的安全机制，主要从完整性保护、内部攻击防护、重放攻击防护、伪造消息防护、重定向防护，以及拒绝服务防护这 6 个方面进行安全性分析。

1）完整性保护：通过数字签名技术对消息中固定对象的摘要进行验证，以此检测是否存在来自外部或内部的消息篡改攻击，进而保护信令消息的完整性。

2）内部攻击防护：采用反馈比较的方法，防止非法节点对重要可变对象或参数进行恶意篡改，保证实际操作与请求业务的一致性。

3）重放攻击防护：为数据包消息引入序列号并添加时间戳，防范节点对信令消息的重放攻击，即使企图延后重放，接收者也可根据时间戳的大小来判断该数据包是否过时。

4）伪造消息防护：通过对信令消息进行数字签名以确保其准确性，防止接收者对错误数据做进一步的处理。

5）重定向防护：数据包到达后首先要进行身份认证，不合法的数据包将被直接丢弃。数据包即使被攻击者重定向，非法的接收者也会因没有相应的密钥解密而使数据得到保护。

6）拒绝服务防护：当非法用户发送大量绑定申请数据包时，由于首先需要进行身份认证，身份不合法的请求将被直接丢弃。即使个别攻击者通过了身份认证，也会因没有提前协商好的密钥无法操作而被丢弃，从而达到对拒绝服务攻击的双重防范。

由以上 6 个方面的安全性分析可知，该机制在安全性上是可靠的。为了对该机制有一个综合的评判，笔者受相关研究思想[23]的启发设计了一个通用的度量模型。该模型假设整个网络有 n 个通信节点，其构成的集合为$\{N_1,N_2,N_3,\cdots,N_n\}$，$N_o$ 为源节点（origin node），N_d 为目的节点（destination node），并且所有节点均符合通信交互过程中所要求的完整性、保密性和可用性等。该模型采用安全满足度、阻塞率满足度和时延满足度为机制度量因素，不同使用者可根据自身实际应用需求进行度量因素的增加、删除与更改，进而得到一个更贴切的度量标准。节点 N_o 和 N_d 之间的安全连接（SC）表示为 $R_{SC}(N_o,N_d)$，节点 N_o 和 N_d 之间满足度量因素的安全连接度量值表示为 $D_{SC}(N_o,N_d)$，度量值的计算如下所示

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

式中：$\sum_o^d$ 为遍历源节点到目的节点的所有节点；V_S 为安全满足度；V_B 为阻塞率满足度（因阻塞率为 P_B，所以 $V_B=1-P_B$）；V_D 为时延满足度；w_1、w_2 和 w_3 分别为以上三个度量因素所对应的权重，并且满足限制条件 $w_1+w_2+w_3=1$。

4　综合分析与实验仿真

4.1　综合分析

此安全身份认证加密机制主要用于完成通信节点之间的首次认证绑定和非首次认证绑定过程，因此选取 CAM（Child-proof Authentication for

MIPv6)、RR(Return Routability)、CGA-RR 和 EBU(Early Binding Update)4 个相关的现有方案[24]，从通信效率、平均时延和防地址伪造等方面进行理论上的综合对比分析，对比结果如表 1 所示。

表 1　与相关方案的理论对比结果

Table 1　Results of comparison with related schemes in theory

Scheme	Communication efficiency	Anti-address forgery	Average delay	Average cost
CAM	Higher	No	Medium	Smaller
RR	Medium	No	Small	Medium
CGA-RR	Low	Yes	Large	Large
EBU	Medium	Yes	Small	Medium
CH-CNA	High	Yes	Small	Small

由表 1 中的对比结果可知，已有的其他方案都存在安全性、效率和开销等不能兼顾的问题。CAM 方案虽然采用了非对称加密算法对报文进行保护，但未对地址的可达性进行验证，不能防止地址伪造。同时，由于每次认证都要使用非对称加密算法，导致平均开销较大。RR 方案虽然对地址可达性进行了验证，但未采用加密算法对密钥的生成进行保护，存在管理密钥被窃听者计算出的风险。CGA-RR 方案在首次绑定中与 CH-CNA 方案具有同样的开销和时延，但在非首次绑定时，平均时延和开销就会因为多次使用非对称加密算法而远大于 CH-CNA 方案。EBU 方案通过预先绑定避免了身份认证带来的较大时延，但平均开销仍然较大。CH-CNA 机制除了具有上述对比方案的优势外，还遵循了原有的 OpenFlow 协议的信息交互方式，无需额外的信令开销，符合轻量级的定义。

4.2　实验仿真

为了进行实验评估，使用 Java 语言对 CGA 算法进行了实现，并对原有的结合算法 RSA[25]和使用的替换算法 ECC 进行了比较。通过设置相关参数，计算首次认证绑定过程中 CGA 算法的哈希值生成时间，并对每组安全级别测试 20 次后取平均值，对比结果如图 9 所示。同时，通过 OMNeT++网络仿真软件搭建了典型的软件定义光网络应用场景[26]，从阻塞率和平均认证绑定时间两个方面，对 CH-CNA 认证绑定机制、SSL/TLS 认证机制和返回路由可达(RRP)认证机制[27]在不同约束条件下进行了对比。该实验场景包含一个 OpenFlow 控制器和 12 个 OpenFlow 交换机节点，并且每个节点下挂载 10 个用户终端，构成了一个三层的树形网络拓扑结构。上下行链路速率均设置为 10 GB/s，控制器到 OpenFlow 交换机的距离设置为 50 km，OLT 到 ONU 的距离设置为 20 km，对比结果如图 10、图 11 所示。

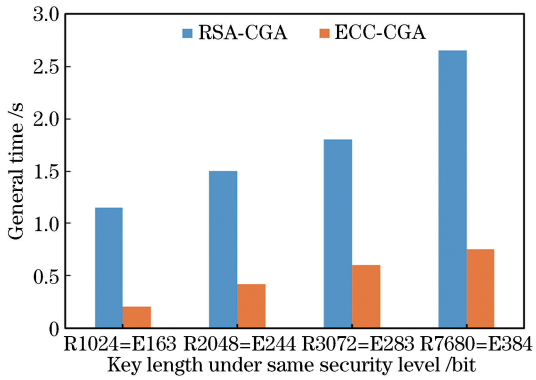

图 9　不同安全强度下的哈希值生成时间比较

Fig. 9　Comparison of hash generation time under different security strengths

由图 9 可知，随着安全强度的增加，RSA 和 ECC 的密钥长度都增加了，但 RSA 密钥长度呈指数增加，而 ECC 密钥长度呈线性增加。此外，当安全强度相同时，如 1024 位长度的 RSA 密钥安全强度等同于 163 位长度的 ECC 密钥安全强度(R1024=E163)，即 ECC 算法具有较短的密钥长度，且用于生成 CGA 的哈希值时间要远短于 RSA 算法。

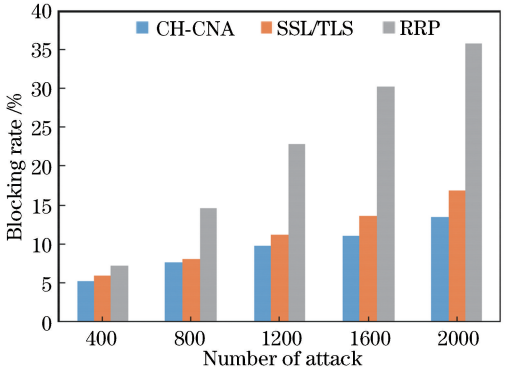

图 10　不同攻击次数下的阻塞率比较

Fig. 10　Comparison of blocking rates under different attack times

在阻塞率方面，由图 10 的对比结果可知，随着攻击次数的增加，阻塞率均增大了，但 CH-CNA 机制要明显优于其他两个方案，且更优于 RRP 认证机制。这是因为 RRP 认证机制仅通过哈希运算实现的是单向身份认证，更容易受到攻击的威胁，导致信令处理的混乱和资源的非法占用，从而造成连接的建立失败，进而引起较高的阻塞率。

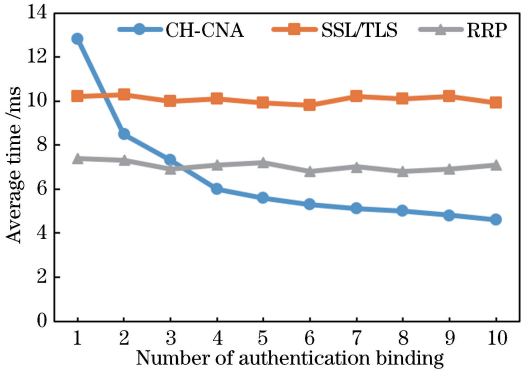

图 11　不同认证绑定次数下的平均耗时

Fig. 11　Average time spent under different authentication binding times

在平均耗时方面，图 11 的对比结果显示 CH-CNA 机制只有在首次认证绑定时用时较多，是因为其采用的是非对称加密算法且涉及密钥协商，发生的消息交互较多。随着认证绑定次数的增加，非首次认证绑定占据的比例也就越大，同时，非首次认证绑定过程采用的是对称加密算法和改进的 HGA 算法，无需过多的消息交互，简化了认证绑定过程。因此，CH-CNA 机制的平均耗时会随着交互次数的增加而逐渐降低，直至接近单次非首次认证绑定的时间，从而达到提高通信效率、减少平均开销的目的。

5　结　　论

针对 OpenFlow 光接入网通信过程中高安全性和低开销难以兼顾的问题，提出了一种轻量级安全身份认证加密机制。在通信双方无共享密钥的情况下，采用非对称加密算法 ECC 算法和 CGA 算法，协商公共密钥完成首次认证绑定。采用对称加密算法和 HGA 算法，以较为简化的过程完成非首次认证绑定。仿真结果表明：与近年来主流的 SSL/TLS 认证加密机制相比，该机制认证绑定时长降低了 53.5%，阻塞率降低了 20.3%；该机制中采用的 ECC-CGA 算法与常规的 RSA-CGA 算法相比，在哈希值生成时间上降低了 72.3%。随着软件定义技术在光接入网方面的广泛应用，以后工作中需要持续深入研究的重点将是设备间的安全通信问题以及因引入安全机制所导致的高代价问题。

参　考　文　献

[1] Rubio-Loyola J, Galis A, Astorga A, *et al*. Scalable service deployment on software-defined networks[J]. IEEE Communications Magazine, 2011, 49(12): 84-93.

[2] Yang H, Zhang J, Zhao Y L, *et al*. Experimental demonstration of remote unified control for open flow-based software-defined optical access networks [J]. Photonic Network Communications, 2016, 31(3): 568-577.

[3] Akhunzada A, Ahmed E, Gani A, *et al*. Securing software defined networks: taxonomy, requirements, and open issues [J]. IEEE Communications Magazine, 2015, 53(4): 36-44.

[4] Chen R R, Kuang C X, Ma J J, *et al*. Algorithm of coherent optical orthogonal frequency division multiplexing-passive optical network system based on optical-comb wave[J]. Acta Optica Sinica, 2017, 37(7): 0706003.
陈荣荣, 邝彩霞, 马俊洁, 等. 基于光梳状波的相干光正交频分复用-无源光网系统的算法[J]. 光学学报, 2017, 37(7): 0706003.

[5] Khondoker R, Larbig P, Senf D, *et al*. AutoSecSDNDemo: demonstration of automated end-to-end security in software-defined networks [C]// 2016 IEEE NetSoft Conference and Workshops (NetSoft), June 6-10, 2016, Seoul, Korea. New York: IEEE, 2016: 347-348.

[6] Chen M, Qian Y F, Mao S W, *et al*. Software-defined mobile networks security [J]. Mobile Networks and Applications, 2016, 21(5): 729-743.

[7] He D B, Padhye S, Chen J H. An efficient certificateless two-party authenticated key agreement protocol [J]. Computers & Mathematics With Applications, 2012, 64(6): 1914-1926.

[8] Potthast M, Forler C, List E, *et al*. Passphone: outsourcing phone-based web authentication while protecting user privacy[M]//Brumley B, Röning J. Secure IT systems. NordSec 2016. Lecture notes in computer science. Cham: Springer, 2016, 10014: 235-255.

[9] He D B, Zeadally S, Kumar N, *et al*. Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(9): 2052-2064.

[10] Zhou Y W, Yang B, Zhang W Z. An improved two-party authenticated certificateless key agreement protocol[J]. Chinese Journal of Computers, 2017, 40

(5): 1181-1191.
周彦伟, 杨波, 张文政. 一种改进的无证书两方认证密钥协商协议[J]. 计算机学报, 2017, 40(5): 1181-1191.

[11] Gao T H, Guo N, Zhu Z L. Access authentication for HMIPv6 with node certificate and identity-based hybrid scheme[J]. Journal of Software, 2012, 23(9): 2465-2480.
高天寒, 郭楠, 朱志良. 节点证书与身份相结合的HMIPv6网络接入认证机制[J]. 软件学报, 2012, 23(9): 2465-2480.

[12] Jiang H, Zhang L Q, Ruan L L. Study on public key cryptography-based 802.1x bidirectional authentication [J]. Computer Applications and Software, 2016, 33(2): 290-293.
蒋华, 张乐乾, 阮玲玲. 基于公钥密码体制的802.1x双向认证研究[J]. 计算机应用与软件, 2016, 33(2): 290-293.

[13] Wang M M, Liu J W, Chen J, *et al*. Software defined networking: security model, threats and mechanism[J]. Journal of Software, 2016, 27(4): 969-992.
王蒙蒙, 刘建伟, 陈杰, 等. 软件定义网络: 安全模型、机制及研究进展[J]. 软件学报, 2016, 27(4): 969-992.

[14] Wang T, Chen H C, Cheng G Z. Research on software-defined network and the security defense technology[J]. Journal on Communications, 2017, 38(11): 133-160.
王涛, 陈鸿昶, 程国振. 软件定义网络及安全防御技术研究[J]. 通信学报, 2017, 38(11): 133-160.

[15] Fu Y H, Bi J, Zhang K Y, *et al*. Scalability of software defined network [J]. Journal on Communications, 2017, 38(7): 141-154.
付永红, 毕军, 张克尧, 等. 软件定义网络可扩展性研究综述[J]. 通信学报, 2017, 38(7): 141-154.

[16] Zhang L. The study of security technology of access network based on SDN [D]. Beijing: Beijing University of Posts and Telecom, 2014: 9-17.
张磊. 基于SDN的接入网安全技术研究[D]. 北京: 北京邮电大学, 2014: 9-17.

[17] Benabbou J, Elbaamrani K, Idboufker N, *et al*. Software-defined networks, security aspects analysis [C]//2015 11th International Conference on Information Assurance and Security (IAS), December 14-16, 2015, Marrakech, Morocco. New York: IEEE, 2015: 79-84.

[18] Sayid J, Sayid I, Kar J. Certificateless public key cryptography: a research survey[J]. International Journal of Security and Its Applications, 2016, 10(7): 103-118.

[19] Cui J H, Zhang Y Z, Wang Z, *et al*. Light-weight object detection networks for embedded platform[J]. Acta Optica Sinica, 2019, 39(4): 0415006.
崔家华, 张云洲, 王争, 等. 面向嵌入式平台的轻量级目标检测网络[J]. 光学学报, 2019, 39(4): 0415006.

[20] Aura T. Cryptographically generated addresses (CGA)[M]//Boyd C, Mao W. Information security. ISC 2003. Lecture notes in computer science. Berlin, Heidelberg: Springer, 2003, 2851: 29-43.

[21] Rajendran T, Sreenaath K V. Hash optimization for cryptographically generated address [C]//2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE'08), January 6-10, 2008, Bangalore, India. New York: IEEE, 2008: 365-369.

[22] Zhang S J, Lan J L, Hu Y X, *et al*. Survey on scalability of control plane in software-defined networking[J]. Journal of Software, 2018, 29(1): 160-175.
张少军, 兰巨龙, 胡宇翔, 等. 软件定义网络控制平面可扩展性研究进展[J]. 软件学报, 2018, 29(1): 160-175.

[23] Lara A, Ramamurthy B. OpenSec: policy-based security using software-defined networking[J]. IEEE Transactions on Network and Service Management, 2016, 13(1): 30-42.

[24] Guo Z Q, Wang Z X, Zhang L C, *et al*. An efficient and secure route optimisation scheme for mobile IPv6 based on Hash generate address [J]. Computer Applications and Software, 2016, 33(6): 105-109.
郭志强, 王振兴, 张连成, 等. 基于Hash生成地址的移动IPv6高效安全路由优化方案[J]. 计算机应用与软件, 2016, 33(6): 105-109.

[25] Li X L, Ai W J. On a security binding mechanism based on identity authentication of communication nodes [J]. Computer Applications and Software, 2015, 32(1): 294-296, 308.
李向丽, 艾文君. 一种基于通信节点身份认证的安全绑定机制的研究[J]. 计算机应用与软件, 2015, 32(1): 294-296, 308.

[26] Azodolmolky S, Petersen M N, Fagertun A M, *et al*. SONEP: a software-defined optical network emulation platform [C]//2014 International Conference on Optical Network Design and Modeling, May 19-22, 2014, Stockholm, Sweden. New York: IEEE, 2014: 216-221.

[27] Eidgahi S Z, Rafe V. Security analysis of network protocols through model checking: a case study on mobile IPv6 [J]. Security and Communication Networks, 2016, 9(10): 1072-1084.