基于预分配密钥的无线Mesh网络认证研究

李俊涛

（中共青海省委党校，青海西宁 810001）

【摘要】随着高速网络时代的到来，无线Mesh网络作为一种新型的无线网络架构，已受到越来越多的关注，移动用户在网络路由器认证切换过程中延时较大问题也日益凸显。为了提升移动用户的用网体验，文章提出了一种新的高效切换认证协议，该协议在椭圆曲线密钥协议的基础上，结合用户历史认证切换记录的概率，将切换密钥预分发给目标路由器，实现无线Mesh网络的高效切换认证。最后通过实验对比，进一步验证了该协议优于其他研究协议，为今后无线Mesh网络认证研究提供了一定的参考。

【关键词】Mesh网络；切换认证；预分配秘钥

【doi:10.3969/j.issn.2095-7661.2022.03.002】

【中图分类号】TN929.5 【文献标识码】A 【文章编号】2095-7661(2022)03-0004-04

Research on Wireless Mesh Network Authentication Based on Pre-distributed Key

LI Jun-tao

(Party School of Qinghai Provincial Committee of CPC, Qinghai, Xining, China 810001)

Abstract: With the advent of the high-speed network era, wireless mesh network, as a new wireless network architecture, has received more and more attention. The problem of large delay of mobile users in the process of network router authentication and handover has become increasingly prominent. In order to improve the network experience of mobile users, this paper proposes a new efficient handover authentication protocol. Combined with the probability of user history authentication handover record, the handover key is pre distributed to the target router to realize efficient handover authentication of wireless mesh network. Finally, through experimental comparison, it is further verified that this protocol is superior to other research protocols, which provides a certain reference for the future research of wireless mesh network authentication.

Keywords: mesh network; switching authentication; pre-distributed key

无线Mesh网络作为一种新型的无线网络架构，近年来受到越来越多的关注，通过相邻节点多跳方式接入，支持单点对单点、多点对多点，是一种高容量、高速率、自匹配能力强、覆盖范围广的分布式网络。随着无线网络技术的高速发展，用户对网络服务质量提出了更高的要求，为确保计算机网络的安全高效运行，确实有效地保护用户隐私，最大限度地减少切换时延，本文提出了一种安全高效的切换认证协议，将椭圆曲线的Diffie-Hellman(DH)密钥协议和Mesh网络用户的历史认证切换记录相结合，利用概率算法将切换密钥预分发给Mesh路由器，用户根据消息认证码只需两次握手就能完成切换认证的过程，从而大幅度提升了网络认证效率，提高了网络服务质量。

1 椭圆曲线的Diffie-Hellman密钥协商协议

本文所设计的切换认证协议，主要采用的是密码学中椭圆曲线DH密钥协议，该协议已被广泛应用在与网络信息安全研究相关领域[1]。假设q为素数(q>3)，F_q是有限素数域，E/F_q是定义在F_q上的椭圆曲线，P是椭圆曲线上的点以q为阶，G是由P构成的循环加法群，Z_q^*是小于q的一个整数集。选择一个随机数$x \in Z_q^*$，计算$X = xP$是相对简单的，

[收稿日期] 2022-07-13

[作者简介] 李俊涛(1982—)，男，河南淅川县人，中共青海省委党校高级工程师，本科，研究方向：网络信息安全。

反之想要从X和P的值，算出x是困难的[2]，在这一特性的基础上运用DH算法，使两个用户可以安全地交换秘钥，具体的执行过程如下：用户甲选择密钥$x \in Z_q^*$，得到$X = xP$，并将X通过公开信道发送给用户乙；用户乙选择密钥$y \in Z_q^*$，得到$Y = yP$，并将Y通过公开信道发送给用户甲；甲根据乙发送过来的Y计算双方的协商密钥$SSK_1 = xY = x(yP) = xyP$；乙根据甲发送过来的X计算双方的协商密钥$SSK_2 = yX = y(xP) = xyP$；甲乙两个用户之间共享密钥$SSK_1 = SSK_2$。

2 改进用户预测认证路由协议

本文所设计的协议主要分为：网络初始化阶段、移动用户预测阶段、密钥预分发阶段以及认证阶段。

2.1 网络初始化阶段

首先认证服务器（AS）会生成自己的公私钥对，然后为每个无线Mesh路由器（MR）生成对应身份信息的私钥，用户端（UC）则需要向AS发送自己的身份信息进行网络注册[3]，整个过程如图1所示，具体步骤如下：

1）AS根据椭圆曲线的DH密钥协商协议，随机选择一个参数$x \in Z_q^*$作为私钥，得到公钥$P_{pub} = xP$，然后应用散列函数$H_1:\{0.1\}^* \times G \rightarrow Z_q^*$，$H_2:\{0.1\}^* \rightarrow Z_q^*$，生成消息认证函数$Hkey(m)$，其中$m$为消息，$key$为密钥。最终获得系统参数$\{q, E/Fq, P, G, H_1, H_2, Hkey(m), P_{pub}\}$。

2）MR将身份信息$IDmr$发送给AS，AS收到身份信息后，选择随机数$y \in Z_q^*$，计算$Y_{MR} = yP$，$h_{MR} = H_1(ID_{MR} \| Y_{MR})$和$sk_{MR} = y + xh_{MR}$，然后将$h_{MR}$和$sk_{MR}$通过安全信道发送给MR进行保存，并得到MR的公钥为$sk_{MR}P$。

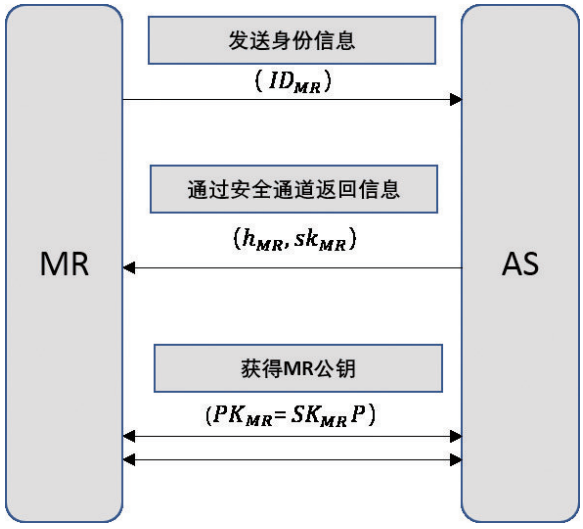

图1　MR获得密钥的过程图

2.2 移动用户预测阶段

每当用户端(UC)进行切换认证，AS都会将切换记录存入UC对应的记录表内，以此来作为历史拓扑信息。此记录表的信息包含：当前接入的MR，切换后接入的NMR，以及接入时间等。UC在首次接入Mesh网络后，AS会根据UC的身份信息和记录表信息，计算UC从当前连接的MR切换到下一个MR（NMR）的概率，并将结果发送给新的NMR，然后将切换密钥发送给切换概率高的相邻路由器。切换矩阵如图2所示，UC历史切换拓扑生成的详细过程如下：

1）确定时间间隔T，UC的切换行为与其行动轨迹相关，由于不同时间段的行动轨迹不同，切换到不同路由器的概率也不尽相同。因此可以根据不同的时间段来预测UC移动轨迹，进而更加准确判断出UC即将连接的路由器。时间间隔T的值由网络系统的性能决定，因为T越短意味着AS需要存储的记录表就越多。本文根据常规活动规律设置时间间隔T为6小时，每个UC则对应拥有4个记录表，分别为：0点—6点、6点—12点、12点—18点、18点—24点。每当UC完成切换事件，AS就会将该事件完成的时间记录到该UC的切换记录表中。

2）根据时间间隔T，每个UC都对应4个切换矩阵，如图2所示。假设无线Mesh网络中有N个路由器（MR1,MR2……MRN），矩阵中的第i行第j列的数值表示UC从MRi切换到MRj发生的次数，相同路由器(MRk)的切换和不相邻路由器发生切换事件的值为0。当用户端(UC)进行切换认证，AS会将切换记录存入UC对应的记录表内，然后在每个固定时间周期更新矩阵，更新周期由网络系统性能确定。

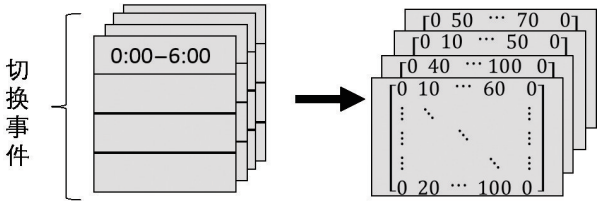

图2　切换矩阵图

3）预测UC的行动轨迹，当UC完成认证接入网络后，会将自身ID_{UC}发送给当前连接的MRi，再由MRi将自身ID_{MRi}会同ID_{UC}以及当前的时间发送给AS。AS根据这些信息找出UC对应矩阵的第i行数据进行计算，得出从MRi到其他路由器的概率，根据概率的高低选择N个概率高的路由器，发送ID_{MRi}和切换密钥。当UC连接到新的路由器后，新

的路由器会重复上述步骤，将下一轮的切换密钥发送给下一个路由器。

2.3 密钥预分发阶段

UC在完成首次身份认证接入网络时会与当前接入的MR_i共享会话密钥(SSK)，以确保会话的安全性[4]。在用户预测阶段完成后，AS将需要预分发的N个相邻路由器信息发送给当前MR_i，MR_i通过会话密钥SSK与UC进行交互，并将切换密钥分发给和它相邻的路由器，详细过程如下：

1）UC选择随机数$x,y \in Z_q^*$，得到$X = xP$，$Y = yP$，通过会话密钥SSK生成密文$\beta = \mathrm{Enc}_{SSK}(X,Y)$发送给当前$MR_i$，$MR_i$接收到消息后，使用会话密钥$SSK$解密得到$X$、$Y = \mathrm{Des}_{SSK}(\beta)$，同时用自己的私钥为$X$、$Y$进行数字签名$\gamma = \mathrm{Sig}_{SK_{MR_i}}(X,Y,ID_{UC})$，并使用公钥$PK_{MR_k}$依次对选出的N个相邻路由器签名进行加密$\delta = \mathrm{Enc}_{PK_{MR_k}}(\gamma,X,Y,ID_{UC},t1)$，其中$t1$为时间戳，最后将这些信息发送给$MR_k$。

2）MR_k在收到消息后进行解密获得$(\gamma,X,Y,ID_{UC},t1)$，同时验证时间戳$t1$是否有效，如果无效就直接丢弃，反之验证签名γ是否有效，如果有效就保存切换密钥X、Y。

2.4 切换认证阶段

伴随着UC的移动，连接到路由器的通信质量会随之改变，当网络通道质量降低到一定的阀值后，为了获得更好的网络服务，UC就需要选择新的通道质量更好的MR进行连接。当切换到并连接到新的合法的MR时，UC需要确认MR的身份，同时MR也要确认UC身份的合法性[5]，整个切换认证过程如图3所示，具体步骤如下：

1）首先UC选择时间戳T_{UC}，计算消息$m=(T_{UC}, ID_{UC}, ID_{MR})$，根据切换密钥$X$、$Y$计算消息认证码$MAC_{UC} = H_X(m)$，最后计算切换认证消息$Auth = MAC_{UC} \oplus X$，将$(Auth,T_{UC},ID_{UC},ID_{MR})$，发送给MR请求接入网络。

2）当MR接收到UC发送过来的消息后，首先验证T_{UC}时间戳是否有效，如果有效就继续，否则就拒绝，接着根据ID_{UC}获得切换密钥X和Y，根据切换密钥X计算$MAC_{MR} = H_X(m)$，根据认证消息$Auth$和X计算$MAC_{UC} = Auth \oplus X$，并判断两个MAC是否相等，如果不等则拒绝该切换请求，否则允许接入网络证明该UC是合法的。最后通过切换密钥Y生成该路由器的认证消息$Auth_{MR} = MAC_{UC} \oplus Y$，将回应消息$(Auth_{MR},ID_{UC},ID_{MR})$发送给UC。

3）当UC接收到来自路由器MR的回应消息后，进行反向验证，根据认证消息$Auth_{MR}$和切换密钥Y获得$MAC_{MR} = Auth_{MR} \oplus Y$，判断两个MAC是否相等，如果相等就接入网络，否则就拒绝接入当前MR。

4）整个认证过程结束后，UC根据当前接入的MR的公钥计算会话密钥$SSK = xPK_{MR}$，MR根据保存的切换密钥X，计算$SSK = sk_{MR}X$。上述过程中，如果MR中的切换密钥X失效，用户UC则需要进行传统身份认证。

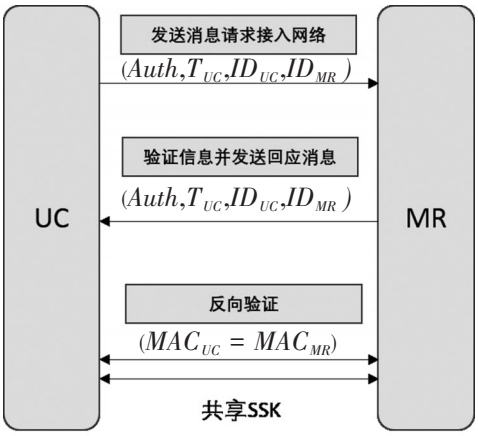

图3 切换认证过程图

3 安全性分析

无线Mesh网络切换认证协议的设计还需要满足以下五个方面的安全性要求，以保障切换认证环境与用户信息的安全分别是：双向认证，密钥协商安全性，数据完整性，可撤销性和抗攻击性[6]。

双向认证：在整个过程中用户UC和目标路由器MR都必须互证自身的合法性。文中提到的密钥预分发阶段中，MR获得的切换密钥是通过会话密钥加密后随机产生的。所以攻击者无法获取准确的切换密钥，在整个切换认证过程中，只有合法的UC才能将身份信息和对应的验证信息发送给MR，只有当验证信息通过后，UC才会被认定为合法的。对于MR来说，切换密钥是上一个合法路由器使用自己的公钥加密后发送的，只有合法的MR才能解密得到切换密钥X、Y。当MR使用正确的切换密钥Y，才能计算出正确的回应消息，当正确的回应消息通过UC认证时，才能证明该MR的合法性，这样就达到了双向互证的目的。

密钥协商安全性：认证过程中的会话密钥SSK，只有合法的UC和MR能计算得出，UC是根据切换密钥X和MR的公钥计算得出，MR是根据切换密钥Y和MR的私钥计算得出。整个过程中切换密钥是随机选取的，MR的私钥是AS通过安全信道发送过来的，整个预分发的过程又是建立在椭

圆曲线算法密钥交换协议上的，所以能有效保障会话密钥协商的安全性。

数据完整性：在整个切换认证过程中，UC和MR的通信中都包含各自的消息认证码，只有消息认证码完整无缺，通信才能成立，故此消息认证码能有效地保障数据的完整性。

可撤销性：UC在接入网络后，每次认证切换的历史信息和其身份信息都会保存在认证服务器中，若UC在使用网络过程中进行了违法操作，或者网络服务时限过期，认证服务器可以随时取消认证，不再为其提供网络服务。

抗攻击性：攻击者通过捕获工具可以轻易窃听到切换认证过程中的通信数据并进行相关的攻击。但是本文所提出的协议，通信数据包是通过会话密钥*SSK*加密的，没有*SSK*是无法获取真正的通信内容。同时通信数据包中都加入了时间戳的要素，如果攻击者利用重放切换认证消息来进行攻击，首先会检查时间戳是否有效，无效就拒绝连接。其次在验证认证消息*Auth*时也有时间戳信息，只有两次的时间戳信息一致才能通过。所以本文提出的协议能够有效地防范非法攻击。

4 实验与分析

Mesh网络认证协议不仅要保障切换过程的安全性，还要保障切换过程的高效性。从有效减少网络认证用时出发，本文主要考虑4个方面：握手的次数、消息验证时长（Mac）、哈希函数计算时长(Hash)和异或(Xor)所产生的延时。通过实验采用Python3.7.3中各类函数运算，在同一环境下（Win10,Inter Core i7-8700K 3.7 GHz）对上述可计算的三个方面进行运算，延时结果如表1所示。

表1　运算延时表

运算	延时
Mac	0.032 ms
Hash	0.013 ms
Xor	0.004 ms

结合上述运算结果同文献[7]、文献[8]所提出的高效认证协议的性能进行比较，得出切换认证总延时对比，如表2所示。

表2　各协议性能分析比较表

运算/协议	文献[7]	文献[8]	本文
Mac	0.032 ms*4次	0.032 ms*2次	0.032 ms*2次
Hash	0.013 ms*1次	0.013 ms*10次	0.013 ms*0次
Xor	0.004 ms*0次	0.004 ms*0次	0.004 ms*4次
延时总时长	0.141 ms	0.194 ms	0.080 ms
握手次数	3次	2次	2次

从上表可以看出，文献[7]中的协议总共需要3次握手，而本文的协议只需要2次握手，与之相比本文提出的协议具有更小的计算代价和通信代价，切换效率更加明显。而与文献[8]提出的协议相比，虽然二者都需要2次握手，但是本文提出的协议延时总时长仅需0.08 ms,计算代价明显较小，所以也具有更高的效率。综上所述，通过对以上4个方面的综合对比，能够证明本文提出的切换认证协议具有较小的计算代价和通信代价，切换效率更高，具备一定的研究价值。

5 结语

为了改善无线Mesh网络中移动用户的服务体验，本文提出了一种基于椭圆曲线Diffie-Hellman的用户预测网络切换认证协议。认证服务器通过预测用户的行动轨迹，将切换密钥预分发给用户即将连接的路由器，提前做好认证连接准备，有效减少用户连接网络的等待时间。通过安全性分析和实验证明，本文提出的协议具备良好的安全性能和较低的计算代价，能够有效地完成认证切换。该协议通过降低网络的通信代价、路由器的存储代价和切换认证的时延，提升了用户体验，使得无线Mesh网络的认证性能得到了进一步加强。

【参考文献】

[1]魏伟,陈佳哲,李丹,张宝峰.椭圆曲线Diffie-Hellman密钥交换协议的比特安全性研究[J].电子与信息学报,2020(8):1820-1827.

[2]王辈,胡红钢.基于椭圆曲线中配对的密码学研究综述[J].密码学报,2022(2):189-209.

[3]张耀辉.PPPoE网络协议的安全性分析[J].湖南邮电职业技术学院学报,2017(4):24-26.

[4]罗旬,严承华.Mesh网络中基于节点信誉度和标识的可信认证[J].信息技术,2016(6):40-44.

[5]孙中杰.基于速率切换的BLE Mesh网络路由转发协议[J].物联网技术,2021(11):35-37.

[6]张钧媛,郑小芳.基于预认证的无线Mesh网络快速切换认证技术方案[J].现代电子技术,2015(1):83-86.

[7]谭涛.基于凭证的无线Mesh网络快速认证的技术研究[D].恩施：湖北民族学院,2018.

[8]Amit Kumar Roy, Ajoy Kumar Khan. Efficient Authentication and Key Management Scheme for Wireless Mesh Networks[J]. International Journal of Internet Technology and Secured Transactions,2019(1-2)：184-200.