文章编号：1007-5321(2017)增-0058-05 DOI:10.13190/j.jbupt.2017.s.013

身份与位置分离网络中的可证明三元认证接入协议

姚 苏[1,2]， 关建峰[3]， 潘 华[1]， 张宏科[2]

(1. 中国航空综合技术研究所，北京 100028；2. 北京交通大学 电子信息工程学院，北京 100044；
3. 北京邮电大学 网络技术研究院，北京 100876)

摘要：针对身份与位置分离网络中接入协议的安全问题，提出一种可证明的三元认证接入协议，实现了所有通信实体(终端、接入交换路由器和认证服务器)的双向认证，有效地防止了未授权终端的接入，防止了伪造的认证服务器和非法的接入交换路由器. 通过对 Ballare-Rogaway 模型的扩展和性能分析可知，该协议基于 BR 扩展模型是可证明安全的.

关 键 词：身份与位置分离网络；三元认证；可证明安全；接入协议

中图分类号：TP393 **文献标志码**：A

Provably Secure Three-Elements Peer Access Authentication Protocol in Identifier/Locator Separation Network

YAO Su[1,2]， GUAN Jian-feng[3]， PAN Hua[1]， ZHANG Hong-ke[2]

(1. Hina Aero-Polytechnology Establishment, Beijing 100028, China;
2. School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044, China;
3. Insisitute of Network Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: Aiming at assuring the authenticity and creditability of the terminals in identifier/locator separation network, a provably secure three-elements peer access authentication protocol (PSTAAP) protocol was proposed. This protocol realized mutual authentication among all the communicating entities in the network (including terminal, access switch network and authentication center). It can effectively block unauthorized terminals to access the network, and can prevent unauthentic authentication center and access switch router from cheating the terminal. It was verified that this protocol was provably security based on Ballare-Rogaway extended model and performance analysis.

Key words: identifier/locator separation network; three-elements peer authentication; provably secure; access protocol

身份与位置分离网络作为未来网络技术重要技术解决方案，可以解决传统网络中带来的安全性问题. 但是，与传统网络一样，为了保证网络的安全，终端在接入网络都需要采取一定的安全认证手段进行保护. 然而，在传统网络中的二元安全认证方式在安全性、灵活性和效率上存在一些问题. 因此，针对以上问题，提出基于身份与位置分离网络的三元认证协议，从而保证身份与位置分离网络中终端认证的安全性.

郑等[1]提出的一体化网络中可证明的安全接

收稿日期：2016-05-11

基金项目：国家重点基础研究发展计划项目(2013CB329102)；国家科技重大专项项目(2013ZX03006002)；国家自然科学基金项目(61471029)

作者简介：姚 苏(1986—)，男，博士生，E-mail:yaosu@bjtu.edu.cn；张宏科(1957—)，男，教授，博士生导师.

入认证协议(PSAAP, provably secure access authentication protocol),没有实现终端和接入交换路由器之间的双向认证.提出安全接入三元认证协议(PSTAAP, provably secure three-elements peer access authentication protocol)实现了所有通信实体的双向认证,有效地防止了未授权的终端接入,防止了伪造的认证服务器,以及非法的接入交换路由器.通过 BR 模型的扩展,证明该协议基于 Ballare-Rogaway(RB)扩展模型是可证明安全的.

1　身份与位置分离网络的模型

国内外诸多研究机构开展了身份位置分离网络技术的研究工作,主要研究成果包括:基于主机身份与位置分离的方案,如主机身份协议[2](HIP, host identify protocol),以及基于网络的身份与位置分离方案,如位置身份分离协议[3](LISP, locator/identifier separation protocol)、一体化网络体系结构[4]等.提出的协议正是采用网络的身份与位置分离方案.其中,接入交换路由器(ASR, access switch router)位于接入网的边缘,负责连接接入网和核心网,完成接入标识和路由标识的分离映射.认证服务器(AC, authentication center)位于核心网的服务层,为接入终端和接入交换路由器提供接入认证和授权服务.认证服务器的数据库中存有注册过的接入终端或接入交换路由器的认证信息,并实时监听认证请求.收到认证请求后在既定的认证算法下核实认证者的可信性,最后将认证结果返回接入交换路由器.

2　PSTAAP 协议

提出的可证明安全三元认证接入协议 PSTAAP,如图 1 所示,其通信流程如下.

1)接入路由器 ASR 生成随机数 R_{ASR},连同它的身份标识信息 ID_{ASR} 发给终端 MN,激活本次接入鉴别流程.

2)终端 MN 收到 ASR 发送的 R_{ASR} 和 ID_{ASR} 后,生成随机数 R_{MN},并使用自己的私钥 $PrivK_{MN}$ 对 R_{ASR}、R_{MN}、ID_{MN} 签名生成身份认证消息 $[R_{ASR}、R_{MN}、ID_{MN}]PrivK_{MN}$,连同终端的身份标识信息 ID_{MN} 一起发送给接入交换路由器 ASR.

3)接入交换路由器收到终端 MN 请求认证的消息后,生成随机数 R'_{ASR},连同终端 MN 和接入路由器 ASR 的身份标识 ID_{MN} 和 ID_{ASR},以及随机数 R_{MN} 发送给认证服务器 AC 请求认证.

4)所有的身份认证都由认证服务器 AC 来完成,当 AC 收到 ASR 提交的身份认证请求后,根据 ID_{MN} 和 ID_{ASR} 分别搜索 MN 和 ASR 的有效公钥 $PubK_{MN}$、$PubK_{ASR}$,并验证 MN 和 ASR 的身份.验证成功向 ASR 发送认证成功响应分组,包括 PAA 和 PAN,其中 PAA 为 AC 的私钥 $PrivK_{AC}$ 对 R'_{ASR}、ID_{MN}、$PubK_{MN}$ 的签名,PAN 为 AC 的私钥 $PrivK_{AC}$ 对 R_{MN}、ID_{ASR}、$PubK_{ASR}$ 的签名.

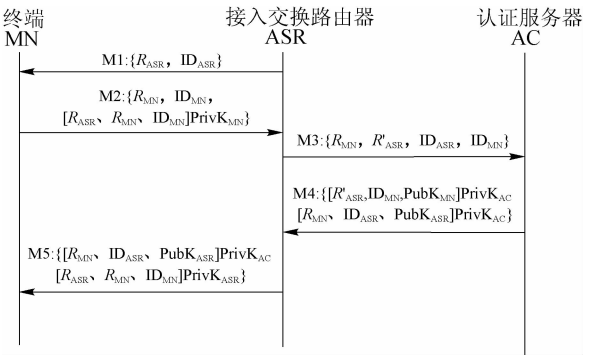

图 1　PSTAAP 协议通信流程

ASR 收到身份认证响应分组后,首先通过 AC 的公钥 $PubK_{AC}$ 判断 PAA 中的随机数 R'_{ASR} 和步骤 3 中发送的随机数 R'_{ASR} 是否一致来验证 PAA,从而 ASR 验证了 AC 的合法性;然后利用 PAA 中 $PubK_{MN}$ 解开步骤 2)中收到的认证消息 $[R_{ASR}、R_{MN}、ID_{MN}]PrivK_{MN}$,校验与步骤 1 中发送的 R_{ASR},从而完成 ASR 对 MN 的合法性的验证.

5)ASR 使用自己的私钥 $PrivK_{ASR}$ 对 R_{ASR}、R_{MN}、ID_{MN} 签名生成身份认证消息 $[R_{ASR}、R_{MN}、ID_{MN}]PrivK_{ASR}$,连同从 AC 收到的认证消息 PAN 发送给 MN;MN 收到消息后,首先通过用 AC 的公钥 $PubK_{AC}$ 解开 AC 发送的验证消息 $[R_{MN}、ID_{ASR}、PubK_{ASR}]PrivK_{AC}$,校验与步骤 2)中发送的 R_{MN},从而完成 MN 对 AC 的合法性验证;根据获取 $PubK_{ASR}$ 解开 ASR 发送的验证消息 $[R_{ASR}、R_{MN}、ID_{MN}]PrivK_{ASR}$ 获得 R_{MN},校验与步骤 1)中发送的 R_{MN},若一致,完成 MN 对 ASR 的合法性验证.

3　PSTAAP 协议安全性证明

可证明的安全性理论在协议的安全性形式化证明中得到了广泛的应用,比较有代表性的是 BR93 模型和 BR95 模型[5].笔者设计的 PSTAAP 协议中共有 4 类实体,分别是攻击者、终端、接入交换路由器和认证服务器.因此,需要扩展 BR93 和 BR95 中

的协议模型,给出适用于本协议的安全三元认证协议定义.

定义1 如果PSTAAP协议是安全的三元认证协议,那么对任意的多项式时间攻击者需要同时满足如下4个条件.

1)如果协议中接入交换路由器和认证服务器的会话,即oracles $\phi^s_{\mathrm{ASR,AC}}$和$\varphi^t_{\mathrm{AC,ASR}}$具有匹配会话,那么它们都可以转到接受状态.

2)如果协议中终端和认证服务器的会话,即oracles $\psi^s_{\mathrm{MN,AC}}$和$\varphi^t_{\mathrm{AC,MN}}$具有匹配会话,那么它们都可以转到接受状态.

3)如果协议中终端和接入交换路由器的会话,即oracles $\psi^s_{\mathrm{MN,ASR}}$和$\phi^t_{\mathrm{ASR,MN}}$具有匹配会话,那么它们都可以转到接受状态.

4)不匹配会话的概率是可忽略的.

下面针对该定义给出相关证明.

定理1 如果λ是伪随机函数序列,那么基于λ的PSTAAP协议是一个可证明安全三元认证协议.

如果证明基于伪随机函数序列λ的PSTAAP协议是一个安全的三元认证协议,只需证明该协议满足定义1的4个条件,即以下所述的引理1~引理4.

引理1 如果协议中ASR和AC的会话,即oracles $\phi^s_{\mathrm{ASR,AC}}$和$\varphi^t_{\mathrm{AC,ASR}}$具有匹配会话,那么它们都可以转到接受状态.

证明 按照PSTAAP协议的描述,如果协议的交互过程中存在良性攻击,那么攻击者也不会破坏线路中的消息,只是忠实转发线路上的各种消息.因此,在协议结束时ASR和AC都会转到接受状态.引理1得证.

引理2 如果协议中终端MN和AC的会话,即oracles $\psi^s_{\mathrm{MN,AC}}$和$\varphi'_{\mathrm{AC,MN}}$具有匹配会话,那么它们都可以转到接受状态.

证明 按照PSTAAP协议的描述,如果协议的交互过程中存在良性攻击,那么攻击者也不会破坏线路中的消息进行破坏,只是忠实转发线路上的各种消息.因此,在协议结束时终端MN和AC都会转到接受状态.引理2得证.

引理3 如果协议中终端MN和ASR的会话,即oracles $\psi^s_{\mathrm{MN,ASR}}$和$\phi'_{\mathrm{ASR,MN}}$具有匹配会话,那么它们都可以转到接受状态.

证明 按照PSTAAP协议的描述,如果协议的交互过程中存在良性攻击,那么攻击者也不会破坏线路中的消息进行破坏,只是忠实转发线路上的各种消息.因此,在协议结束时终端MN和ASR都会转到接受状态.引理3得证.

引理4 PSTAAP协议中存在不匹配会话的概率是可忽略的.

证明 在这里,只针对oracles $\phi^s_{\mathrm{ASR,AC}}$和$\varphi^t_{\mathrm{AC,ASR}}$的情况,oracles $\psi^s_{\mathrm{MN,AC}}$和$\varphi^t_{\mathrm{AC,MN}}$、$\psi^s_{\mathrm{MN,ASR}}$和$\phi^t_{\mathrm{ASR,MN}}$的情况类似.

这里需要考虑2个试验,第1个实验为真实试验,即攻击者F与PSTAAP协议交互运行的试验,在该试验中,使用密钥K控制下的伪随机函数U_K.第2个试验为随机试验.在该随机试验中,引入随机函数$E:\{0,1\}^{\leqslant L(k)}\rightarrow\{0,1\}^k$,使得$[X]_p=(X,E(X))$.在一个给定输入的情况下,随机函数输出的结果是$\{0,1\}^k$上均匀分布的比特串.认证服务器和接入交换路由器之间不再共享密钥K.当$E=U_K$时,随机试验等同于真实试验.

结论1 在随机试验中发生攻击成功的概率至多为$2^{-k}T(k)$.($T(k)$是攻击者是k的一个多项式函数,表示攻击者查询oracle次数的上限值).按照PSTAAP协议的通信流程,在时间τ_0,ASR发送消息流$(R_{\mathrm{ASR}},\mathrm{ID}_{\mathrm{ASR}})$;在时间$\tau_1$,MN接收消息流$(R_{\mathrm{ASR}},\mathrm{ID}_{\mathrm{ASR}})$;在时间$\tau_2$,ASR接收消息流$(R_{\mathrm{MN}},\mathrm{ID}_{\mathrm{MN}},[R_{\mathrm{ASR}},R_{\mathrm{MN}},\mathrm{ID}_{\mathrm{MN}}]_q)$;在时间$\tau_3$,MN接收消息流$([R_{\mathrm{MN}},\mathrm{ID}_{\mathrm{ASR}},\mathrm{PubK}_{\mathrm{ASR}}]_q,[R_{\mathrm{ASR}},R_{\mathrm{MN}},\mathrm{ID}_{\mathrm{MN}}]_q)$.

如果协议会话发起端MN、ASR和会话M,在没有匹配会话的情况下,那么MN和ASR转到接受状态的概率至多为$2^{-k}T(k)$.

假设在时间τ_1,$\psi^s_{\mathrm{MN,ASR}}$会话收到消息流$(R_{\mathrm{ASR}},\mathrm{ID}_{\mathrm{ASR}})$,并且对$\phi^t_{\mathrm{ASR,MN}}$响应$(R_{\mathrm{MN}},\mathrm{ID}_{\mathrm{MN}},[R_{\mathrm{ASR}},R_{\mathrm{MN}},\mathrm{ID}_{\mathrm{MN}}]_q)$.如果$\phi^t_{\mathrm{ASR,MN}}$转到接受状态,那么在时间$\tau_3$,$\psi^s_{\mathrm{MN,ASR}}$必然收到$([R_{\mathrm{MN}},\mathrm{ID}_{\mathrm{ASR}},\mathrm{PubK}_{\mathrm{ASR}}]_q,[R_{\mathrm{ASR}},R_{\mathrm{MN}},\mathrm{ID}_{\mathrm{MN}}]_q)$的消息流.如果没有任何会话曾经输出过这个消息流,那么敌手能正确计算该消息流的概率至多为2^{-k}.如果确实存在会话曾经输出过该消息流,那么根据$([R_{\mathrm{MN}},\mathrm{ID}_{\mathrm{ASR}},\mathrm{PubK}_{\mathrm{ASR}}]_q,[R_{\mathrm{ASR}},R_{\mathrm{MN}},\mathrm{ID}_{\mathrm{MN}}]_q)$的形式可得出输出该消息流的会话必定是$\phi^t_{\mathrm{ASR},h}$.$\phi^t_{\mathrm{ASR},h}$与

敌手交互具有如下形式：

$$(\tau_0,\lambda,(R'_{\mathrm{ASR}},\mathrm{ID}_{\mathrm{ASR}}))$$

$$(\tau_2,(R'_{\mathrm{MN}},\mathrm{ID}_{\mathrm{MN}},[R'_{\mathrm{ASR}},R'_{\mathrm{MN}},\mathrm{ID}_{\mathrm{MN}}]_q))$$

$$([R'_{\mathrm{MN}},\mathrm{ID}_{\mathrm{ASR}},\mathrm{PubK}'_{\mathrm{ASR}}]_q,[R'_{\mathrm{ASR}},R'_{\mathrm{MN}},\mathrm{ID}_{\mathrm{MN}}]_q)$$

针对以上消息流，存在一个会话 $\psi^{v}_{h,\mathrm{ASR}}$ 可能输出 $(R'_{\mathrm{MN}},\mathrm{ID}_{\mathrm{MN}},[R'_{\mathrm{ASR}},R'_{\mathrm{MN}},\mathrm{ID}_{\mathrm{MN}}]_q$ 的概率至多为 2^{-k}. 如果 $(v,h)\neq(\mathrm{MN},s)$，那么 $[R_{\mathrm{MN}},\mathrm{ID}_{\mathrm{ASR}},\mathrm{PubK}_{\mathrm{ASR}}]_q=[R'_{\mathrm{MN}},\mathrm{ID}_{\mathrm{ASR}},\mathrm{PubK}'_{\mathrm{ASR}}]_q$ 的概率至多为 $2^{-k}(T(k)-2)$，因此 $([R'_{\mathrm{MN}},\mathrm{ID}_{\mathrm{ASR}},\mathrm{PubK}'_{\mathrm{ASR}}]_q,[R'_{\mathrm{ASR}},R'_{\mathrm{MN}},\mathrm{ID}_{\mathrm{MN}}]_q)$ 使得 $\psi^{s}_{\mathrm{MN},\mathrm{ASR}}$ 接受的概率至多为 $2^{-k}(T(k)-2)+2^{-k}+2^{-k}=2^{-k}T(k)$. 因此，结论 1 得证.

当在 ϕ 和 φ、ϕ、ψ、φ、ψ 之间存在的攻击者为良性攻击者时，所用的匹配对话序列组都会让接入终端、接入交换路由器和认证服务器的状态机最终转到接受状态，而存在异常会话的概率为 $p(z)=1-(1-2^{-k}T(K))(1-2^{-k}T(K))(1-2^{-k}T(K))$ 可见，协议的异常会话概率 $p(z)\to 0$. 由此得出 PSTAAP 协议中存在不匹配会话的概率是可忽略的. 引理 4 得证. 由引理 1 ~ 引理 4 得出定理 1 得证. 因此，PSTAAP 协议可以提供足够强度的安全性，是可证明的安全认证三元协议.

4　性能分析

性能评估用到的参数及含义见表 1.

表 1　性能评估用到的参数及含义

参数	含义	参数	含义
(.)	协议标识符	$C^{(.)}_{\mathrm{auth}}$	每跳路由的传输开销
λ	认证请求到达的速率	C_S	协议的认证开销
$T^{(.)}_{\mathrm{auth}}$	协议的认证时延	C_N	随机数生成的开销
P	消息在节点等待和服务时间	C_{V}	密钥验证的开销
$T_{W/L}$	无线/有线链路的传输时延	C_{US}	一对值加解密的开销
T_{AU}	认证服务器的处理时间	C_{HASH}	一次 Hash 运算的开销
T_N	随机数的生成时间	L_C	无线链路带宽
$S_{W/L}$	消息在可靠的无线/有线链路上成功传输的时延	B_W	有线链路带宽
t_W	链路中检测分组丢失检测时间	B_L	消息的发送时延
T_{US}	一对值加解密消耗的时间	α	无线链路的消息传输时延
T_{Hash}	一次 *Hash* 运算的消耗时间	β_w	有线链路的消息传输时延
T_V	密钥生成的时间	β_L	消息的处理时延

1）认证时延

认证时延即移动节点 MN 发出认证请求时间到接受认证响应的时间间隔，包括消息在节点等待和服务时间，链路传输时延以及认证处理时间. 其中，链路传输时延包括无线链路传输时延和有线链路传输时延两部分. 因此，

$$T^{(.)}_{\mathrm{auth}}=P+T_W+T_L+T_{\mathrm{AU}} \tag{1}$$

有线链路可靠性较高，不需要考虑数据包分组丢失情况，因此，T_L 值与 S_L 值相同. 无线链路则需要考虑检测分组丢失的时延. 因此，

$$T_W=2S_W+t_W \tag{2}$$

然而，消息从发送端发送到接收端所需总时延包括消息发送时延、消息传输时延和消息处理时延.

$$S_{W/L}=\alpha+\beta_{W/L}+\gamma=\alpha+L_C/B_{W/L}+\gamma \tag{3}$$

认证处理时间包括随机数生成时间、加解密消耗时间、Hash 运算消耗的时间以及密钥生成时间.

$$T_{\mathrm{AU}}=T_N+T_{\mathrm{US}}+T_{\mathrm{Hash}}+T_V \tag{4}$$

因此，可以得出所提出的安全接入认证协议 PSTAAP 的认证时延为

$$T^{\mathrm{PSTAAP}}_{\mathrm{auth}}=(6P+3T_N+3(2S_W+t_w)+2S_L+12T_{\mathrm{US}}+5T_V)\lambda$$

安全接入三元认证方法 PSTPAP 的认证时延为

$$T^{\mathrm{PSTAAP}}_{\mathrm{auth}}=(7P+4T_N+3(2S_W+t_w)+3S_L+15T_{\mathrm{US}}+5T_{\mathrm{Hash}}+3T_V)\lambda$$

2）认证开销

认证开销 $C^{(.)}_{\mathrm{auth}}$ 定义为每次认证过程中信令开销与处理开销之和.

所提出的安全接入认证协议 PSTAAP 的认证开销为 $C^{\mathrm{PSTAAP}}_{\mathrm{auth}}=(5C_S+3C_N+12C_{\mathrm{US}}+5C_V)\lambda$，安全接入三元认证方法 PSTPAP 的认证开销为

$$C^{\mathrm{PSTAAP}}_{\mathrm{auth}}=(6C_S+4C_N+15C_{\mathrm{US}}+5C_{\mathrm{Hash}}+3C_V)\lambda$$

根据文献[1]所给出的评估参数，可以计算出所提出协议的认证时延和认证开销.

图 2 所示为认证时延随认证请求到达速率 λ 变化的曲线. 2 种认证方法的认证时延都随着 λ 的增大而增加，但是在同等的认证请求到达速率的情况下，笔者提出的 PSTAAP 认证协议相比于 PSAAP 认证协议具有稍大的时延，这是因为 PSTAAP 认证协议中终端和接入交换路由器之间双向认证过程中增加了部分时延.

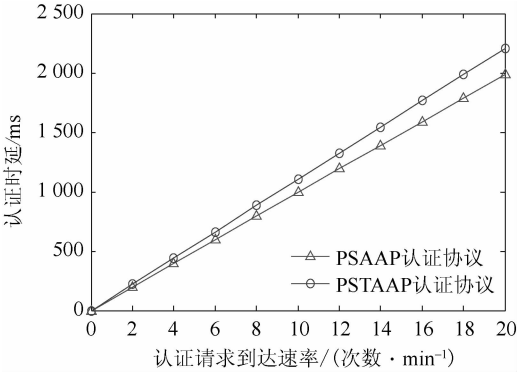

图2 认证时延随认证请求到达速率变化的曲线

图3为认证开销随认证请求到达速率 λ 变化的曲线,两种认证方法的认证时延都随着 λ 的增大而增加,但是在同等的认证请求到达速率的情况下,提出PSTAAP认证协议相比于PSAAP认证协议具有稍大的认证开销,这是因为PSTAAP认证协议中终端和ASR之间双向认证过程中增加了开销,但对于提升认证协议的安全性来说,上述代价是可以接受的.

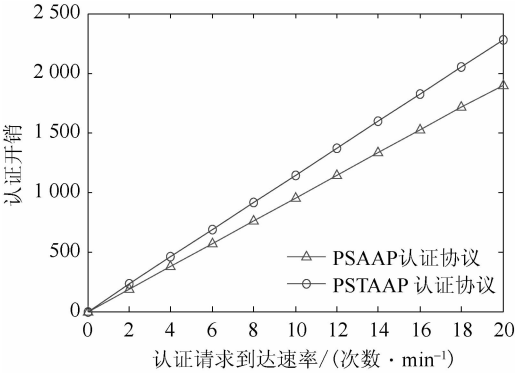

图3 认证开销随认证请求到达速率变化的曲线

参考文献:

[1] 郑丽娟, 韩臻, 徐曼, 等. 一体化网络中可证明安全的三方认证协议[J]. 北京交通大学学报, 2010, 34(5): 26-31.
Zheng Lijuan, Han Zhen, Xu Man, et al. Provably secure three-party authentication protocol in universal network[J]. Journal of Beijing Jiaotong University, 2010, 34(5): 26-31.

[2] Moskowitz R, Farinacci D. Internet draft draft-ietf-hip-rfc4423-bis-11— 2015, Host identity protocol architecture (HIP) [S]. [S. l.]: IETF, 2017: 12-14.

[3] Farinacci D. RFC 6830-2017, The locator/ID separation protocol(LISP)[S]. [S. l.]: IETF, 2013: 9-14.

[4] 董平, 秦雅娟, 张宏科. 支持普适服务的一体化网络研究[J]. 电子学报, 2007, 35(4): 599-606.
Dong Ping, Qin Yajuan, Zhang Hongke. Research on universal network supporting pervasive services[J]. Acta Electronica Sinica, 2007, 35(4): 599-606.

[5] 罗振营, 龙昭华, 陈万东. 基于TePA的以太网链路层安全分析与研究[J]. 计算机应用研究, 2014, 31(6): 1836-1840.
Luo Zhenying, Long Zhaohua, Chen Wandong. TePA-based security analysis and research at Ethernet datalink layer[J]. Application Research of Computers, 2014, 31(6): 1836-1840.