一种可控可信的匿名通信方案

吴振强 周彦伟 乔子芮
(陕西师范大学计算机科学学院 西安 710062)

摘 要 加密技术只能对通信数据的内容进行保护,在电子投票、电子医疗、电子商务和电子现金等一些特殊的应用领域,用户的身份、行为、地理位置等隐私信息的保护程度是评估整个系统安全性的重要因素之一.常用的隐私保护方法是利用匿名通信技术来抵抗窃听和流量分析攻击,但匿名通信技术在增强用户身份等隐私信息保护的同时,恶意用户的身份与行为也受到了匿名保护,如何保护合法用户隐私的同时又能防止恶意行为的攻击是推动匿名通信技术大规模应用的关键.作者以增强计算机安全的可信计算技术为基础,提出一种基于可信平台模块的可控可信匿名通信系统架构,该架构通过群组通信技术实现发送方的身份匿名,在通信链路上采用加密嵌套封装的数据通信方法实现用户行为、地理位置等隐私信息的保护.利用这一框架实现的匿名通信方案是由用户向身份管理中心注册获取群组信息、通过可信性评估的用户从节点服务器下载信任节点、用户用随机选择的信任节点建立匿名通信链路、服务提供方对恶意匿名行为用户的追踪等 4 个功能模块组成.作者对这些模块的协议进行了体系化设计,并给出了每个模块对应的协议方案.通过对方案的安全性、可信性、匿名性、效率等方面的分析与仿真,表明该方案具有较好的安全性、可控性与可信性,可以满足未来互联网环境下大规模部署匿名通信系统的需要.

关键词 匿名框架;匿名认证;可追踪匿名;可信平台模块;平台真实性验证
中图法分类号 TP393 **DOI 号**: 10.3724/SP.J.1016.2010.01686

A Controllable and Trusted Anonymous Communication Scheme

WU Zhen-Qiang ZHOU Yan-Wei QIAO Zi-Rui
(*School of Computer Science, Shaanxi Normal University, Xi'an* 710062)

Abstract Encryption technology can only carry on the protection to the correspondence data content, but in some special application fields, such as e-voting, e-health, e-commerce and e-cash, the protection degree of private information, like user's identity, behavior, geographical location and so on, is one of important attributes to assess the overall system security. The anonymous communication technology that is strongly resistant to both eavesdropping and traffic analysis is the commonly used privacy protection method, but this technology can not only enhance an user's identity information but also protect a malicious user's identity and behavior. How to protect an authorized user's privacy and prevent malicious attacks is the key of promote the large-scale application of anonymous communication technology. A controllable and trusted anonymous communication architecture that build up the computer security with trusted computing based on the trusted platform module is proposed. The architecture realizes the sender's anonymity through a group communication technology, and achieves the protection of privacy information in user behavior, user geographical position by encapsulating package with nested encryptions in communication link. The anonymous communication scheme based on the architecture consists of four functional modules, such as getting group information by the user register for authentication

收稿日期:2010-04-14;最终修改稿收到日期:2010-08-07.本课题得到国家"八六三"高技术研究发展计划项目基金(2007AA01Z438200)、国家自然科学基金重点项目(60633020)资助.**吴振强**,男,1968 年生,博士,副教授,研究方向为匿名通信技术、可信计算、自适应安全、无线网络等. E-mail: zqiangwu@snnu.edu.cn. **周彦伟**(通信作者),男,1986 年生,硕士研究生,研究兴趣为匿名通信技术、可信计算. E-mail: zhouyanwei1986@163.com. **乔子芮**,女,1985 年生,硕士研究生,研究兴趣为智能信息处理.

management center (AMC), trusted user node list that was downloaded from the server after the user have passed the trusted evaluation, established anonymous communication link by randomly selected node, and traceable service of malicious behavior to services provider. This paper has carried on the systematization design to these modules, and gives each module a corresponding protocol. It is shown that the scheme has good security, controllability and credibility by analysis and simulation of safety, dependability, anonymity, and efficiency. The scheme can meet the demand of the large scale deployment of anonymous communication system in the future Internet.

Keywords　anonymity architecture; anonymous attestation; traceable anonymity; trusted platform model; attestation for trustworthiness of computing platform

1 引　言

Internet 作为通信与信息传播的途径正快速发展并且广为人们所接受，与此同时，安全与隐私已成为 Internet 的一个关键问题. 国内外调查机构的民意测验表明用户在使用 Internet 时感到的最大障碍是担心其隐私被破坏[1-2]. 随着加密技术的广泛应用，用户通信数据的安全性得到了保护；然而传统的加密技术很难实现对通信参与者身份的保护，尤其在一些特殊的应用领域，如电子投票、电子医疗、电子商务和电子现金等，用户的身份、行为、地理位置等隐私信息的保护程度是评估整个系统安全性能的重要因素之一，而匿名技术是保护用户隐私的有效方法.

目前，匿名技术已有一定的研究基础，如 Crowds、洋葱路由、Mixnets 等，但对匿名用户的操作存在缺乏监督和控制的不足以及出现利用匿名发动窃听和流量分析攻击时没有相应的应对措施，系统在提供匿名服务的同时降低了其安全性. 匿名技术在发展过程中带来的新问题有[3-4]：恶意分子利用匿名邮件和匿名公告栏系统对他人进行任意的人身攻击和诽谤，或发动反政府言论和邪教活动；犯罪分子利用电子现金系统的匿名性进行非法的重复消费与洗钱行为；恶意分子利用匿名通信系统对服务器发动 DDoS 攻击，或者进行各种非法的网络操作行为，而网络服务提供商与司法机构却难以对其网络 ID 进行有效的历史记录和追踪. 目前，这种通过网络匿名技术所引起的恶意行为的数量在持续增加，其危害程度日益严峻，因此研究网络活动的匿名控制技术及可控匿名系统便成为匿名技术研究的重要内容. 目前的匿名控制技术以及匿名系统存在如下主要问题：(1) 缺乏通用的可控性匿名技术研究. 现有的可控匿名通信系统其设计出发点往往是国家或司法机关的网络监督工具[5]，难以进行商业应用；现有商用匿名控制技术研究与实现主要集中在数据匿名通信范畴内的几个特定应用系统，由于缺乏有效的匿名控制服务支持，反而阻碍了匿名系统的发展与部署. (2) 缺乏可信性匿名技术研究. 目前的匿名通信系统无法与可信平台模块(Trusted Platform Model，TPM)实现交互，同时基于可信计算的匿名通信研究并未引起更多学者的关注. 如 Tor(The Onion Router)匿名通信系统中 Tor 网络节点服务器仅仅依靠传统的安全防护措施对其提供保护，在当前复杂的网络环境下，由于保护措施不足容易使节点服务器成为整个 Tor 匿名通信系统的安全瓶颈；同时新节点在无任何安全性验证的情况下就可以加入 Tor 匿名系统，则加入的恶意节点会对系统的安全性带来危害，使用户的匿名通信过程存在安全隐患.

针对目前匿名技术所面临的诸多问题，本文提出了可控可信的匿名通信方案(Controllable and Trusted Anonymous Communication Scheme，CTACS). CTACS 通过群组通信技术实现发送方的身份匿名，在通信链路上采用加密嵌套封装的数据通信方法实现用户行为、地理位置等隐私信息的保护. 尤其是可信计算的运用使 CTACS 具有更高的安全性、可信性和可控性.

本文第 2 节对相关工作进行介绍；第 3 节给出 CTACS 的框架设计；第 4 节讨论 CTACS 的详细工作流程；第 5 节对 CTACS 框架进行分析；最后对论文的工作进行总结.

2 相关研究工作

2.1 网络的可信性与可控性方面

我国对网络的可信性和可控性有着多年的研究基础，在可信可控网络模型、一体化可信网络及下一代互联网体系结构领域进行了一些前瞻性的研究.

文献[6]认为在可信可控网络体系的研究中要建立一个完整的可信网络,必须解决如下问题:网络与用户行为的可信模型、可信的网络体系、服务的可生存性以及网络的可管理性. 国家"九七三"重点基础研究发展规划项目"一体化可信网络与普适服务体系基础研究"致力于下一代信息网络需求的研究,力求创建一体化可信网络,攻克新一代信息网络及其重大应用的基础性技术[7]. 文献[8]指出下一代互联网体系的研究在国际上还处于起步和规划阶段,同时提出一种可信可控的网络体系结构,基于新体系结构下的网络控制方法,并融合信任管理和不可否认服务等策略给出该体系的可信控制方法. 文献[9]提出的可控网络模型以设置网络中的分布式监测点和监测中心为基础,采用基于特征的网络匿名攻击监测规则,应用攻击源定位算法识别可控网络内部的匿名攻击. 文献[10]针对传统可信网络的不足,结合可信网络关键技术,提出了基于 TPM 的可信网络框架.

国外学者指出下一代网络安全体系应该包含完善的信任机制,需在网络环境下的各实体间建立信任关系,并将信任关系转化为贯穿网络模型的信任链. 2006 年美国国家自然科学基金资助信息空间信任项目,同时美国国家研究委员会也提出信息空间下信任机制研究的建议. 其中,CMU 大学发起的"网络控制与管理的 4D 计划"最具代表性,它致力于网络控制体系及关键问题研究[8,11].

2.2 匿名通信机制方面

我国在低延迟匿名通信系统、匿名度量、动态混淆匿名算法和匿名通信系统评估领域进行了大量研究,取得了一些成果. 文献[12]基于地理多样性和 RTT 路由节点选择算法提出一种分层的基于地理多样性的低延迟匿名通信架构,并给出安全性评估算法. 文献[13]提出基于联合熵的多属性匿名度量模型,该模型实现系统匿名等级隶属度向量的离散化,并给出平衡参数的确定方法. 文献[14]提出适用于无线 Ad Hoc 网络的动态混淆匿名算法,该算法不仅确保了无线 Ad Hoc 节点的匿名性,又解决停等算法的丢包问题. 文献[15]推导出基于重路由匿名通信系统中成员负载的概率公式,并证明成员负载由重路由路径数目以及重路由路径长度的概率分布所决定.

国外的相关研究表明:传统的匿名通信系统对拒绝服务、流量分析等攻击行为的抵抗能力较弱,导致个人隐私信息的威胁增加,制约了匿名通信系统的发展. 为提高可用性及安全性,人们目前正致力于匿名通信系统的可信性等相关研究[16-17].

纵观国内外在可信可控网络体系结构方面的相关研究结果,我们认为非常有必要将匿名通信系统与可信计算技术相结合,以提高匿名通信技术的可信性与可控性,同时,还应加强匿名体系实现技术方面的探讨.

3 CTACS 框架设计

CTACS 框架方案如图 1 所示,其中 Alice 为匿名用户,Bob 为目标主机,Dave 为 CTACS 节点服

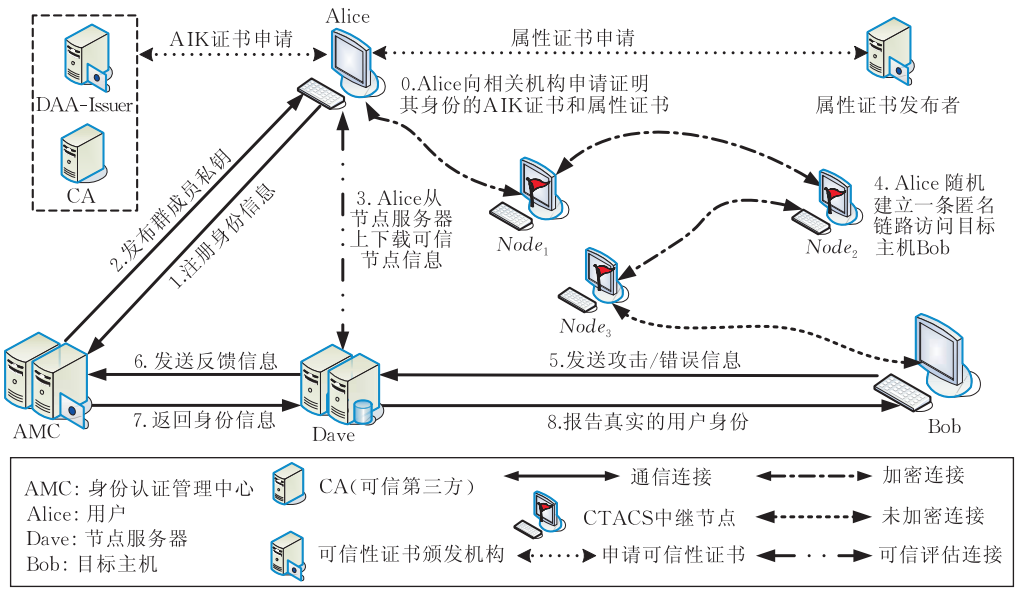


图 1 CTACS 框架结构

务器，AMC（Authentication Management Center，AMC）为身份认证管理中心，CTACS 框架中 AMC 和 Dave 是可信的第三方，具有严格的安全防护措施，且采用服务器并行工作的方式提高工作效率及安全性. 该框架实现了匿名通信的可控操作，对用户的匿名行为建立一条由 Bob 到 Dave，再由 Dave 到 AMC 的追踪机制，通过对用户恶意行为的追踪，实现对用户恶意行为的控制，为用户提供可追踪的匿名服务；同时建立一个完整的从 BIOS 加载、操作系统加载直至接入 CTACS 的信任链传递模型，以 TPM 硬件身份标识为身份证明，实现了基于 TPM 芯片的可信接入认证过程，并实现动态的接入与追踪管理.

如图 1 所描述，CTACS 框架分为 4 个阶段，分别细化为第 0～8 步，共 9 次交互式操作.

3.1　用户到身份管理中心注册

用户在向 AMC 注册前，用户先基于 TPM 进行完整性度量，获得相关可信服务器签发的 AIK 证书和属性证书，即当用户处于安全状态时，才能向 AMC 发出注册请求，AMC 在对用户信息进行验证后，对合法的用户请求进行授权，对其发布可信用户群的成员私钥. 该阶段对应图 1 中的第 0～2 步操作.

3.2　用户下载节点信息

用户得到 AMC 的授权后与节点服务器建立安全可靠的链接，下载一定数目 CTACS 节点的相关信息，并且获得由节点服务器颁发的授权接入证书，在该证书的有效时间内用户持该证书可多次与节点服务器建立可靠的节点下载链路. 该阶段对应图 1 中的第 3 步操作.

3.3　建立可控可信的匿名链接

节点信息下载结束后，用户启动链路建立程序在下载的 CTACS 节点集合中随机选取一个节点协商秘密密钥，最后与它建立一个安全信道. 用户与节点建立安全通道前，节点需要基于 TPM 进行可信性评估，只有通过可信性评估处于安全状态的节点才能和用户建立连接. 密钥建立过程使用短期的 Diffie-Hellman 密钥交换协议，同时使用 TLS 传输协议保证信道的保密性和信息的前向安全，安全信道建立后所有的数据都将通过这个信道进行传输. 同理，用户通过已建立的信道，再继续将匿名连接拓展至其它的节点，并与其协商交换密钥，最终建立一条嵌套加密的匿名链接信道. 数据在传输前首先被用户的代理程序按其所通过节点的顺序从后至前层层加密，在传输过程中，加密后的数据每通过一个节点被解密一次，直到最后一个节点数据被完全解密并转发到目的端. 而数据从目的端返回的过程中，每经过一个节点被加密一次，到达用户后，代理程序又对其进行层层解密，最终转发给用户端的应用程序. 数据在匿名通信链路上传输的过程中，可以利用填充机制使数据包大小保持不变. 由于每个节点仅知道自己的加/解密密钥，对外部攻击者而言，除非他能够获得路径中所有节点的密钥，否则他不可能得到通信数据的明文. 该阶段对应图 1 中的第 4 步操作.

3.4　恶意匿名行为的追踪机制

用户注册和接入阶段的可信性评估过程，在一定程度上杜绝恶意用户的接入，防止恶意匿名行为的出现. 但 CTACS 仍建立对用户恶意匿名访问行为的追踪机制，当目标主机发现用户具有恶意匿名行为时，目标主机将向 AMC 发出追踪用户匿名性的请求，首先目标主机将追踪数据发往节点服务器，对目标机的可信性进行评估，通过评估后，节点服务器将其保存的用户信息连同目标机的追踪信息一起发到 AMC，AMC 基于行为可信性度量机制判断用户匿名行为的可信性，响应对恶意匿名用户的匿名性追踪请求，将恶意用户的身份等注册信息通过节点服务器发往目标主机. 该阶段对应图 1 中的第 5～8 步操作.

4　CTACS 工作流程

4.1　用户注册

图 1 所示，Alice 要建立可控可信匿名连接先到 AMC 进行可信身份注册，获得一个 AMC 所管理群的群成员私钥，在注册前完成完整性度量，将完整性度量值发给证书发布者，获得属性证书 $Cert_{\text{attr}}$，进行平台真实性评估，申请获得 AIK 证书 $Cert_{\text{AIK}}$. 身份注册阶段如图 2 所示，其交互操作主要有

（1）用户首先进行基于 TPM 的完整性度量及平台真实性评估，获得属性证书和 AIK 证书之后，与 AMC 之间基于 SSL 建立安全的通信信道；

（2）用户通过建立的安全信道将个人身份信息及相关证书发给 AMC，AMC 对用户可信平台的可信性进行评估，即 AMC 基于相关策略对 Alice 平台的可信性进行评估，评估过程见论文的 4.3 节；

（3）AMC 验证用户信息的合法性之后，通过安全信道向用户发送其唯一的群成员私钥证书以及群

公钥信息，可采用 SSL 安全协议完成密钥的分发过程.

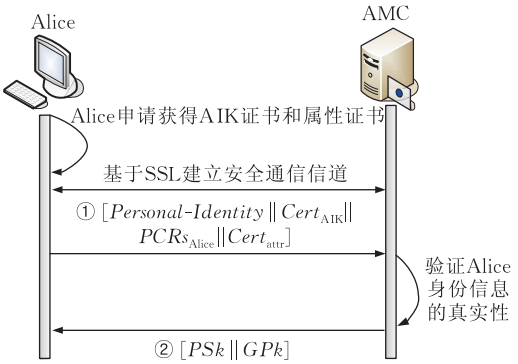


图 2 用户向 AMC 申请注册

注册过程：

① Alice → AMC：RequestHello[$Personal\text{-}Identity \| Cert_{AIK} \| PCRs_{Alice} \| Cert_{attr}$]；

② AMC → Alice：ResponseHello[$PSk \| GPk$]，

其中，$Personal\text{-}Identity$ 是用户个人身份信息，$Cert_{AIK}$ 是 Alice 持有的 AIK 证书，$Cert_{attr}$ 是 Alice 持有的属性证书，$PCRs_{Alice}$ 是 Alice 的完整性度量信息，PSk 是用户的群成员私钥，GPk 是群公钥.

4.2 用户从节点服务器下载可信节点信息

Alice 在 AMC 注册成功后，将与 CTACS 的节点服务器 Dave 建立连接，并下载用户所需的节点信息以建立到达目标机的链路. 通过可信匿名接入认证协议完成 Alice 与 Dave 间的身份合法性认证及平台可信性评估，具体协议流程如图 3 所示.

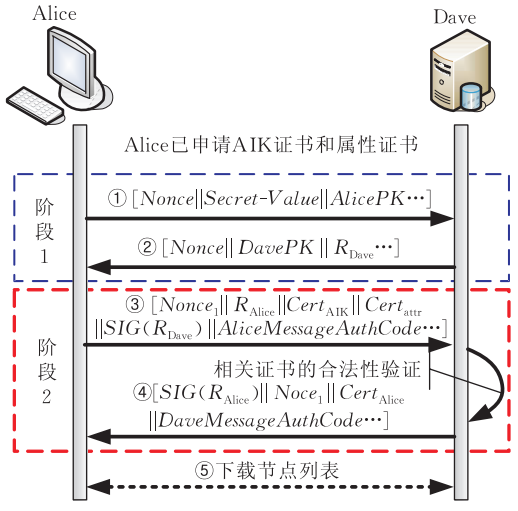


图 3 可信匿名接入认证协议流程

Alice 与 Dave 建立链接时，Alice 已获得 AIK 证书和属性证书. Alice 通过与 Dave 两个阶段的协商建立到 Dave 的安全可靠链接，其中第 1 阶段主要协商产生 Alice 及 Dave 的消息认证码种子，第 2 阶段则进行 Alice 与 Dave 间的双向身份认证及 Dave 对 Alice 平台的可信性评估. Alice 通过身份合法性认证及平台可信性评估后，Dave 为 Alice 颁发授权接入证书，在该证书的有效时间内用户持该证书即可多次与 Dave 建立可靠的节点下载链路. Dave 将 Alice 的相关信息存储到节点数据库中，使其成为 CTACS 的一个节点. 由于在 CTACS 中，AMC 和 Dave 具有严格的安全防护措施，因此对用户信息的安全性同样给予高等级的保护. 具体的链接建立过程为

① Alice → Dave：RequestHello[$Nonce \| SessionID \| GroupList \| CipherSuite \| Secret\text{-}Value \| AlicePublicKey$]；

② Dave → Alice：ResponseHello[$Nonce \| SessionID \| GroupInformation \| CipherSuite \| DavePublicKey \| R_{Dave}$]；

通过 Hello 消息 Alice 与 Dave 进行会话前的协商，$Nonce$ 是由时间戳和随机数组成的一个随机数，用以区分先前发送的消息是否与响应消息相对应，$SessionID$ 是 Alice 与 Dave 间会话的 ID 号，$GroupList$ 是 Alice 所注册的 AMC 群证书列表，$AlicePublicKey$ 是 Alice 的群公钥，$CipherSuite$ 是 Alice 消息认证所支持的会话密钥协商算法如数字签名算法、消息摘要算法等，$Secret\text{-}Value$ 是 Alice 产生的此次通信会话的秘密信息，$DavePublicKey$ 是 Dave 的公钥，R_{Dave} 是 Dave 产生的用于 Alice 签名的随机数.

第 1 阶段协商 Alice 与 Dave 间消息认证码的种子，此两个种子是根据之前的交互信息计算出来的. 在 Hello 消息之后，双方拥有了共享的秘密值 $Secret\text{-}Value$；对于 Dave 有

$$DaveWriteMacSecret = \text{SHA1}(\text{“Dave”} \| \text{RequestHello} \| \text{ResponseHello} \| Secret\text{-}Value);$$

而对于 Alice 有

$$AliceWriteMacSecret = \text{SHA1}(\text{“Alice”} \| \text{RequestHello} \| \text{ResponseHello} \| Secret\text{-}Value);$$

其中 $Secret\text{-}Value$ 是唯一标识一个会话的最重要的秘密信息. 在双方产生各自的消息认证码之后，双方发送的消息都带有消息认证码. 即

$$Message = MessageHead + MessageContent + MessageAuthCode.$$

对于 Alice 有

$$AliceMessageAuthCode =$$

Hash(*AliceWriteMacSecret* ‖ 发送的消息内容)；

对于 Dave 有

DaveMessageAuthCode=

Hash(*DaveWriteMacSecret* ‖ 发送的消息内容)；

③ Alice → Dave：Authentication [*Personal-Identity* ‖ $Time_A$ ‖ $Nonce_1$ ‖ $PCRs_{Alice}$ ‖ $Cert_{AIK}$ ‖ $Cert_{attr}$ ‖ $SIG(R_{Dave})$ ‖ R_{Alice} ‖ *AliceMessageAuthCode*]；

$SIG(R_{Dave})$是用户对节点服务器产生随机数签名操作的签名值，$Time_A$是认证消息发送时间，随机数 $Nonce_1$用以验证之前发送的消息是否得到了相应的回复.

Dave 在接收到 Alice 的度量信息、AIK 证书和属性证书后，对 Alice 平台的可信性进行评估，根据评估结果 *Result* 制定相应的访问控制策略.

④ Dave→ Alice：Response [$Nonce_1$ ‖ *Result* ‖ $SIG(R_{Alice})$ ‖ *DaveMessageAuthCode*]；

$SIG(R_{Alice})$是节点服务器对用户产生随机秘密值签名操作的签名值. 消息验证码确保了消息传输过程的安全性，而通信双方对签名值的验证确保双方身份的真实性.

此时，Alice 与 Dave 间建立安全可靠的节点传输链路，并将用户的身份信息存储到 Dave 相应的数据库中，同时为用户颁发授权接入证书.

⑤ Dave→ Alice：Datatransmission [*Node-List* ‖ $Cert_{Server}$ ‖ *DaveMessageAuthCode*].

其中，*Node-List* 是 Alice 下载的节点信息列表，$Cert_{Server}$是节点服务器颁发的授权接入证书.

4.3　平台的可信性评估

用户 Alice 接入 CTACS 时，对 Alice 平台的可信性进行评估，确保接入 CTACS 的用户安全可信，保证了目标主机 Bob 对 Alice 身份的可信；同时匿名通信链路建立阶段对节点平台的可信评估确保匿名链路的可信性，保证了 Alice 对匿名链路的可信. 可信性评估包括平台 TPM 芯片的真实性验证和平台的完整性验证.

4.3.1　平台真实性验证

在 TCG 制定的 DAA 方案中，DAA 颁发者是一个发布 DAA 签名的权威机构，各个不同的 TPM 厂商都设置有自己的 DAA 颁发者，这样就形成了相对独立的信任域，不同的信任域有不同的 DAA 颁发者，不同信任域内的参与者将信任不同的 DAA 颁发者，导致现有的 DAA 方案只适用于单信任域的情况，当位于不同信任域的验证者和示证者需要交互时，本节给出的跨域匿名认证方案可以完成 Dave 和 Alice 间的匿名认证. 这一过程分为域内匿名认证和域间匿名认证两种情况.

(1) 域内验证

当示证者 Alice 与验证者 Dave 是同一信任域的 TPM 用户时，使用改进的直接匿名认证方案[18]对 Alice 平台的真实性进行验证，具体验证过程如图 4 所示，其中 CA 为可信第三方参与 Alice 与 DAA 证书发布者 DAA Issuer 间密钥的协商.

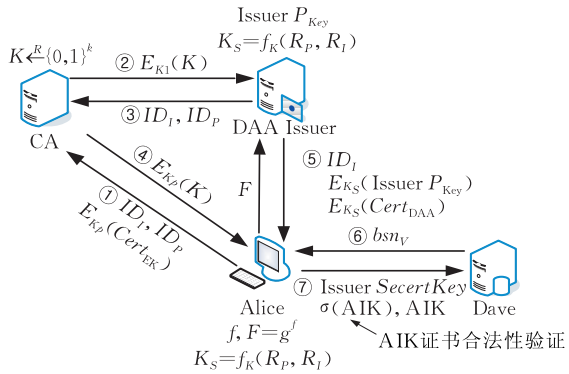


图 4　域内的平台真实性验证过程

Setup 阶段. DAA Issuer 选择阶为素数 q 的两个群 $G_1=\langle g_1\rangle$，$G_2=\langle g_2\rangle$，并选择 G_1 和 G_2 之间的双线性映射 $e: G_1\times G_1\to G_2$，随机选择 $x\leftarrow Z_q$，$y\leftarrow Z_q$，计算 X 和 Y，其中 $X=g_1^x$，$Y=g_1^y$，设置短期公钥 P_{Key}，群私钥 SK_I，并将群公钥作为发布者短期公钥.

Join 阶段. CA 作为可信第三方验证 Alice 发送消息中 MAC 的正确性，验证 $Cert_{EK}$的有效性，如果验证通过，则选择 K 并发送消息(ID_P，ID_I，s，R_P，R_I，$E_{K1}(k)$，$MAC_{K1}(ID_P, ID_I, s, R_P, R_I, E_{K1}(k))$)给 DAA Issuer；DAA Issuer 验证消息中 MAC 的正确性，通过验证后，解密获取 K，计算会话密钥 $K_S=f_K(R_P, R_I)$，同时发送消息(ID_I，ID_P，s，R_I，R_P，$MAC_{K1}(ID_I, ID_P, s, R_I, R_P)$)给 CA；CA 在收到消息后，验证 MAC 的正确性，验证通过后发送消息(ID_I，ID_P，s，R_I，R_P，$E_{Kp}(k)$，$MAC_{Kp}(ID_I, ID_P, s, R_I, , R_P, E_{Kp}(k))$)给 Alice；Alice 收到消息后，验证 MAC 的正确性，验证通过后解密获取 K，计算会话密钥 $K_S=f_K(R_P, R_I)$. 接下来 DAA Issuer利用会话密钥 K_S与 Alice 进行通信，Alice 从 DAA Issuer 处秘密地获得 DAA 证书 $Cert_{DAA}$，并根据 DAA Issuer 的长期公钥和 DAA 种子计算秘密信息 f，并根据发布者短期公钥 *PublicKey* 计算 F.

Alice 在申请接入 Dave 前完成上述两阶段，即 Alice 申请获得 $Cert_{DAA}$证书，申请接入过程中验证 $Cert_{DAA}$证书的合法性.

Sign 阶段. Alice 的安全芯片 TPM 将其 AIK 的公钥用 DAA 证书签名后发给验证者 Dave.

Verify 阶段. Dave 对接收到的消息检验签名的合法性,若验证通过,则确认 Alice 是拥有真实 TPM 芯片的平台.

(2)域间验证

当 Alice 与 Dave 分属不同的信任域时,则通过跨域匿名认证方案完成 Alice 平台的真实性验证,具体验证过程如图 5 所示.

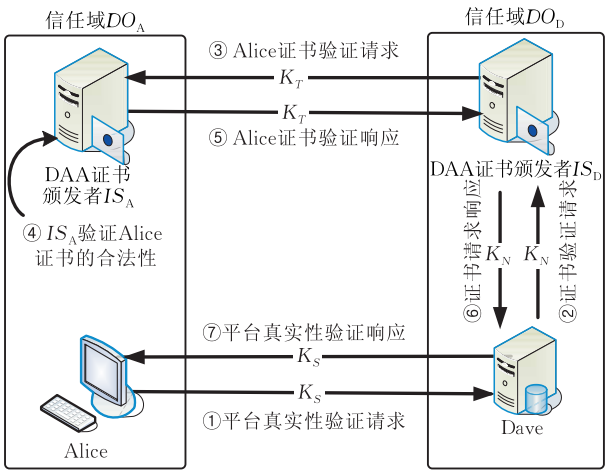


图 5 域间的平台真实性验证过程

假设:信任域 DO_A 和 DO_D 的 DAA 证书颁发者生成的密钥对分别为 $\{K_{PubA}、K_{PrivA}\}$ 和 $\{K_{PubD}、K_{PrivD}\}$;Alice 与 Dave 真实性验证之前,通过协商 Dave 与 Alice 间的会话密钥为 K_S;Dave 与 IS_D 间的会话密钥为 K_N;IS_D 和 IS_A 间的会话密钥为 K_T.

① Alice 向 Dave 发送平台真实性验证请求,该请求中包含 Alice 的完整性度量数据和其所属的域名;

$$Alice \rightarrow Dave: AutRequest = K_S\{DO_A \| DO_D \| Time_1 \| Nonce \| Cert_{AIK} \| PCRs_{Alice}\}$$

Alice 将其所在域的标识 DO_A、验证者所在域的标识 DO_D、请求发送时间 $Time_1$、随机数 $Nonce$、AIK 证书 $Cert_{AIK}$ 和平台完整性度量值 $PCRs_{Alice}$ 用与 Dave 间的会话密钥 K_S 加密后发送给 Dave;

② Dave 接收到 Alice 的验证请求后,向本域中的 DAA 证书颁发者 IS_D 发送证书验证请求,同时发送 Dave 自身的完整性度量信息给 IS_D;

$$Dave \rightarrow IS_D: CertRequest = K_N\{K_{PubD}\{DO_A \| Time_2 \| Cert_{AIK} \| PCRs_{Alice} \| PCRs_{Dave} \| Nonce_1 \| TS_1\}$$

Dave 将收到的 Alice 的请求消息 $\{DO_A \| Cert_{AIK} \| PCRs_{Alice}\}$、证书验证请求发送时间 $Time_2$、时间戳 TS_1、随机数 $Nonce_1$ 及 Dave 平台的完整性度量值 $PCRs_{Dave}$ 用 IS_D 的公钥签名,然后用 Dave 与 IS_D 间的会话密钥 K_N 加密后发给 IS_D. 时间戳用以防止重放攻击,随机数用以验证发送的消息是否回复,公钥加密保证只有 IS_D 才能解密消息.

③ IS_D 向 IS_A 发送 Alice AIK 证书真实性验证请求,同时将 Dave 平台真实性评估结果签名后发送给 IS_A;

$$IS_D \rightarrow IS_A: CertAuthRequest = K_T\{K_{PrivD}\{DO_A \| DO_D \| Cert_{AIK} \| PCRs_{Alice} \| Time_3 \| Nonce_2 \| TS_2 \| Result_{Dave}\}\}$$

IS_D 将收到的 Alice 的完整性度量信息 $PCRs_{Alice}$、AIK 证书 $Cert_{AIK}$、时间戳 TS_2、随机数 $Nonce_2$、请求发送时间 $Time_3$ 及对 Dave 的真实性验证结果 $Result_{Dave}$ 用 IS_D 的私钥签名,然后再用 IS_D 与 IS_A 的会话密钥 K_T 加密后发送给 IS_A,私钥签名确保该消息是 IS_D 所发.

④ IS_A 验证 IS_D 签名信息的真实性,获得 Dave 的真实性验证信息,响应合法 IS_D 的验证请求,完成对 Alice 平台的真实性验证;

⑤ IS_A 将 Alice 平台真实性验证结果 $Result_{Alice}$ 签名后发给 IS_D;

$$IS_A \rightarrow IS_D: CertAuthReplay = K_T\{K_{PrivA}\{ID_A \| Nonce_2 \| Time_4 \| Result_{Alice}\}\}$$

IS_A 为 Alice 赋予一个唯一的 ID 号,该 ID 号相当于用户的一个假名;IS_A 将 Alice 可信性评估结果 $Results_{Alice}$、Alice 的 ID 号 ID_A、真实性验证时间 $Time_4$ 和随机数 $Nonce_2$ 用 IS_A 的私钥签名,然后用 IS_A 与 IS_D 间的会话密钥 K_T 加密后发给 IS_A.

⑥ IS_D 验证 IS_A 签名值的真实性,获得 Alice 平台的真实性验证结果,IS_D 将真实性验证结果签名后发给 Dave;

$$IS_D \rightarrow Dave: CertReplay = K_N\{K_{PrivD}\{ID_A \| Result_{Alice} \| Nonce_1 \| Time_5\}\}$$

IS_D 将 Alice 的 ID 号、Alice 平台真实性验证结果 $Result_{Alice}$、随机数 $Nonce_1$ 及消息应答时间 $Time_5$ 用 IS_D 的私钥签名,然后用 Dave 与 IS_D 间的会话密钥 K_N 加密后发送给 Dave.

⑦ Dave 通过验证 IS_D 签名信息的真实性,即可获知 Alice 平台真实性验证结果 $Result_{Alice}$,完成对 Alice 平台的跨域真实性验证,即 Dave 在 IS_D 和 IS_A 的协助下完成对 Alice 平台的真实性验证.

4.3.2 平台完整性验证

基于属性证书完成对用户平台的完整性验证过程如图 6 所示.

①平台完整性验证请求. Alice 发送完整性验证请求消息 c 给属性证书发布者;

②平台完整性验证响应. 当证书发布者收到 Alice 发送的证书请求消息后,验证 Alice 的合法性,如果其合法,则发送平台完整性信息的消息标识 c' 及 Alice 发送的挑战消息 c 给 Alice;

③ Alice 收到证书发布者发布的平台完整性验证挑战消息后,触发 TPM 进行 PCR 值的获取;

④平台向 TPM 请求获得相应的 PCR 值,并使用私钥对 PCR 值和随机数 c' 进行签名;

⑤平台收集并规格化完整性度量日志,将规格化后的完整性度量日志、Quote 及相关信息以标准的完整性报告格式发送给证书发布者;

⑥证书发布者收到平台发送的完整性信息后,提取出平台的属性信息,并对这些属性信息进行验证,产生相应的证书;

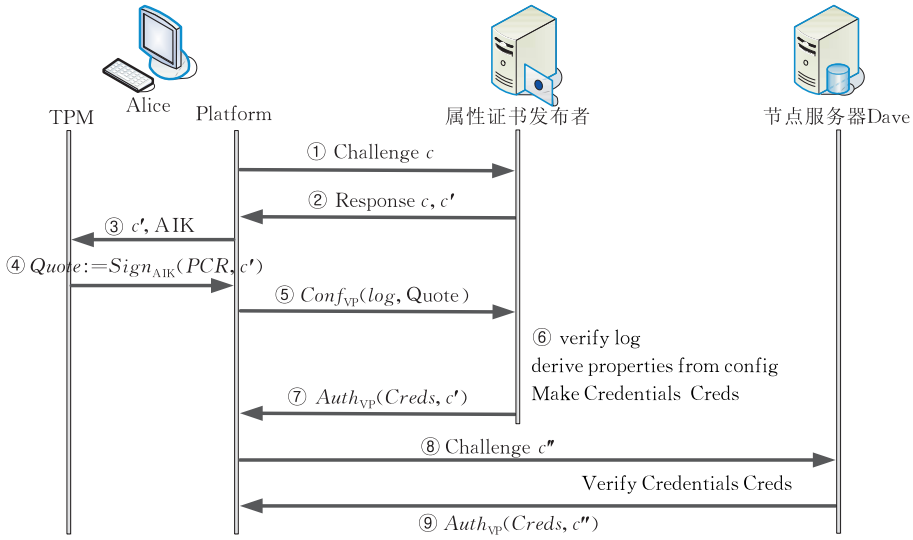


图 6　用户平台完整性验证过程

⑦将构建的属性证书以安全的方式发送给 Alice.

以上步骤在 Alice 申请接入 Dave 前完成，即 Alice 申请属性证书，在 Alice 接入 Dave 过程完成下述两步，即验证属性证书的合法性.

⑧ Alice 获得由证书发布者颁发的属性证书后，持该证书向 Dave 发送完整性验证消息；

⑨ Dave 收到 Alice 发送的属性证书后，基于相应的策略对属性证书中所显示的平台完整性进行验证.

Alice 将完整性度量信息以“推”的模式发送给属性证书发布者，并获得其颁发的属性证书，Dave 通过属性证书验证 Alice 的完整性.

4.4　授权接入证书

4.4.1　证书结构

从 4.3 节中可以看出平台的完整性验证过程比较复杂，若用户频繁地申请接入 CTACS，会导致 CTACS 的工作效率降低，浪费节点服务器的计算能力，同时增加用户 TPM 的完整性度量负载. 为了提高 CTACS 的工作效率，利用授权接入证书以减少通信申请过程的可信性验证次数，证书结构如图 7 所示，在证书的有效授权时间内，用户持该证书即可与 Dave 建立节点下载链路.

有效期	颁发时间	授权对象	签名

图 7　授权接入证书

图 7 中，有效期表示证书的有效授权时间；颁发时间表示证书的颁发时间；授权对象表示证书授权对象的 ID 号；签名表示节点服务器对证书的签名信息.

4.4.2　证书合法性验证

在授权接入证书的有效授权时间内，用户持该证书申请加入可信网络，服务器通过验证授权证书的合法性来判断用户的可信性. 设当前时间为 T_{Now}，通过以下步骤验证证书的合法性：

① 节点服务器首先验证签名信息的有效性，该项检查验证证书颁发者的身份，同时检查证书内容是否被篡改；

② 验证 $T_{\text{NOW}} \leq$ 有效期＋颁发时间是否成立，该项检查验证证书在当前时间是否有效；

③ 验证用户 ID 信息与证书的绑定 ID 是否一致，该项检查验证证书持有者是否是证书的申请者.

若上述验证都通过，即授权接入证书在当前时间有效，表明用户身份的合法及平台的可信.

4.5　建立可控可信的匿名链路

用户下载 CTACS 节点信息成功后，通过这些节点建立一条到达目标主机的可控可信匿名链路.

用户 Alice 同路径中的每个节点协商一个密钥. 连接建立和数据转发过程如图 8 所示，在开始建立通信链路时，Alice 向它选定的第 1 个节点（记为 $Node_1$）发送数据包 *request* 要求 $Node_1$ 首先对自身的安全性进行基于 TPM 安全芯片的完整性度量，$Node_1$ 将完整性度量值通过数据包 *requested* 发送给 Alice，Alice 对节点 $Node_1$ 可信平台进行可信性评估，若节点 $Node_1$ 处于不安全状态，Alice 将选择另一可信节点建立连接；否则 $Node_1$ 处于可信状态，Alice 将发送一个 *create* 数据包给 $Node_1$（用新的 *circID* 来标识其到 $Node_1$ 的链路）. *Create* 数据包的负载包含前一半的 Differ-Hellman 握手信息 g^x，当 $Node_1$ 收到 *create* 数据包后，用 $Node_1$ 自身的公钥加密. $Node_1$ 返回一个 *created* 数据包，其中包含另一半的握手信息 g^y 和会话密钥 $K=g^{xy}$ 的 Hash 值. 一旦链路建立，Alice 和 $Node_1$ 就可以发送和转发数据包，转发数据包用他们协商好的的会话密钥进行加密.

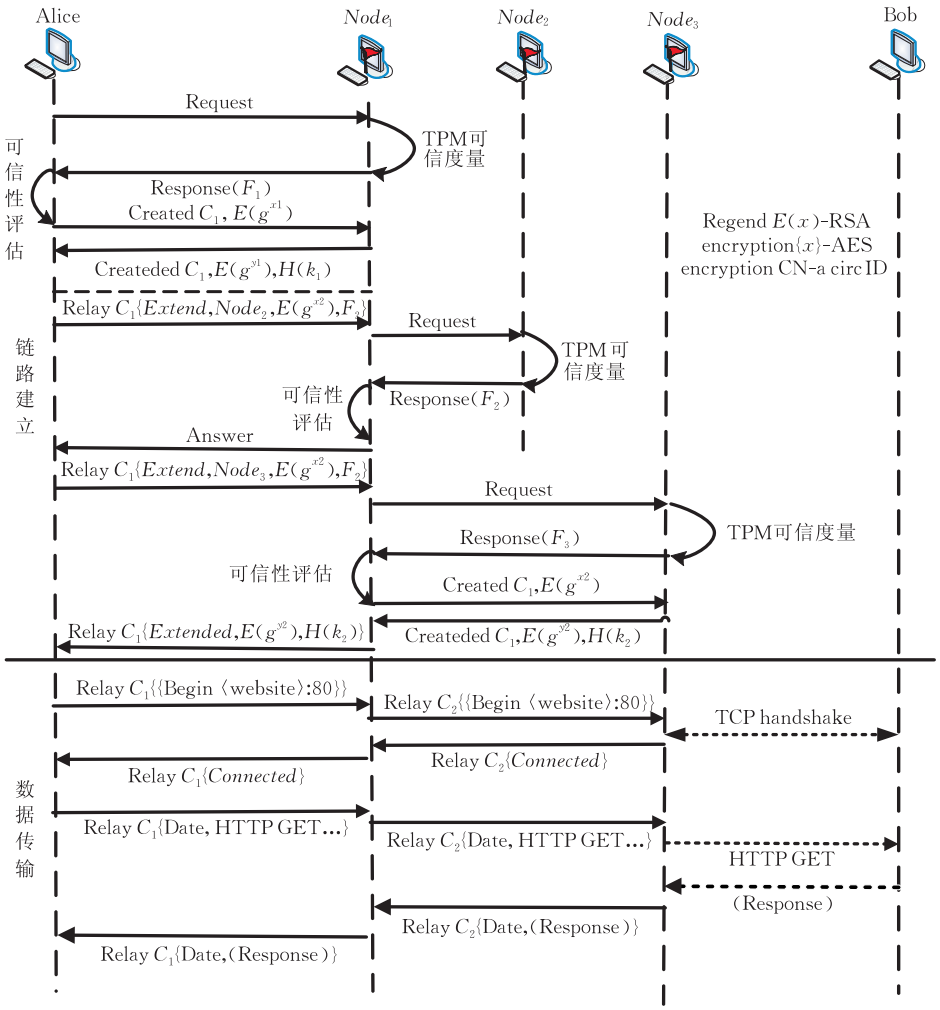


图 8 可控可信匿名链路的建立过程

扩展电路. 为了扩展这条虚电路，Alice 发送一个 *relay extend* 数据包给 $Node_1$，其中包含加密的握手信息 g^{x2} 和下一跳的节点（记为 $Node_2$）的地址及可信性评估授权信息，则 $Node_1$ 向 $Node_2$ 发送数据包 *request* 要求其首先对自身的安全性做可信度量，$Node_2$ 将完整性度量摘要值用数据包 *requested* 发送给 $Node_1$，$Node_1$ 对 $Node_2$ 的可信平台进行可信性评估，若 $Node_2$ 可信性评估没有通过，$Node_1$ 发送数据包 *answer* 给 Alice，告知 Alice 该可信节点处于不安全的状态，则 Alice 将选择另一可信节点扩展连接；否则 $Node_2$ 处于可信的状态，可以通过其建立可信连接，于是 $Node_1$ 复制这一半的握手信息到一个 *create* 数据包中，然后将其发送给 $Node_2$. 由于 $Node_1$ 选择了一个新的 *circID* 用于标识和 $Node_2$ 的连接，Alice 无法知道该 *circID*. 当 $Node_1$ 收到 $Node_2$ 的响应信息后，$Node_1$ 用它与 Alice 之间的会话密钥加密一个 Relay *Extended* 数据包，然后将它发回给 Alice. 现在，这条链路链接到了 $Node_2$，Alice 和 $Node_2$ 的会话密钥为 $K_2 = g^{x2\,y2}$. 将链路延伸至第 3 个节点或更多节点，Alice 只需继续上述过程，告知当前最后一个节点将链路继续拓展并对其授权可信性评估的权力. 这种电路级的握手协议可以实现单向身份认证和单向密钥认证. 单向身份认证是指 Alice 知道自己与哪个 Node 握手，但 Node 并不知道是哪个用户建立的此条链路. 单向密钥认证是指 Alice 和 Node 协商了一个密钥，Alice 仅知道 Node 已获得这个密钥信息.

通过上述方法，Alice 建立了一条到目标主机 Bob 的可控可信的匿名连接，在建立连接的过程中，只有通过可信性评估的中间节点才将其接入电路，否则舍弃该节点，由此可见，Alice 建立的这条可控可信匿名链路中的所有节点都处于安全可信状态，进而保证了整个 CTACS 的可信性和安全性.

链接成功建立后，Alice 的代理程序在传输前将应答数据按其所通过节点的顺序从后至前层层加密，在传输过程中，加密后的数据每通过一个节点被

解密一次，直到最后一个节点数据被完全解密并转发到目的端，各节点在解密的同时进行填充操作使通信数据包的大小保持不变，防止流量分析、窃听等网络攻击. 数据从目的端返回的过程中，每经过一个节点被加密一次，到达 Alice 后又被代理程序层层解密，最终转发给 Alice 的应用程序.

4.5.1　链路建立

Alice→$Node_{(1)}$: Request [*Trusted-Metric-Notice*];

$Node_{(1)}$→Alice:
Response [*TPM-Metric-Information*(F_1)];

Alice→$Node_{(1)}$: Create [$C_1 \| E(g^{x1})$];

$Node_{(1)}$→Alice: Createded [$C_1 \| E(g^{y1}) \| H(k_1)$];

Alice→$Node_{(1)}$: Relay C_1[*Extend* $\| Node_2 \| E(g^{x2}) \| F_2$];

$Node_{(1)}$→$Node_{(2)}$: Request [*Trusted-Metric-Notice*];

$Node_{(2)}$→$Node_{(1)}$:
Response [*TPM-Metric-Information*(F_2)];

$Node_{(1)}$→$Node_{(2)}$: Create [$C_2 \| E(g^{x2})$];

$Node_{(2)}$→$Node_{(1)}$: Createded [$C_2 \| E(g^{y2}) \| H(k_2)$];

$Node_{(1)}$→Alice: Relay C_1[*Extended* $\| E(g^{y2}) \| H(k_2)$].

…

Alice: CTACS 用户，$Node_{(i)}$ ($i=1,2,3,\cdots$): CTACS 第 i 个可信节点，*Trusted-Metric-Notice*: 可信度量通知，*TPM-Metric-Information*(F_i)($i=1,2,\cdots$): 第 i 个节点的可信度量信息，g^{xi} ($i=1,2,\cdots$): Alice 与第 i 个节点协商密钥的前一半 Diffe-Hellman 握手信息，g^{yi} ($i=1,2,\cdots$): Alice 与第 i 个节点协商密钥的后一半 Diffe-Hellman 握手信息.

4.5.2　数据传输

(1) Alice 发送数据

Alice→$Node_{(1)}$: *Send*[$E_{NodeKey(1)}$[$E_{NodeKey(2)}$
[$\cdots$[$E_{NodeKey(n-1)}$[$E_{NodeKey(n)}$[*Data*]]]$\cdots$]]];

$Node_{(1)}$→$Node_{(2)}$: *Send* [$D_{NodesKey(1)}$[$E_{NodeKey(1)}$
[$E_{NodeKey(2)}$[$\cdots$[$E_{NodeKey(n-1)}$[$E_{NodeKey(n)}$[*Data*]]]$\cdots$]]]];

$Node_{(1)}$ 对接收到的数据用与 Alice 的会话密钥解密后，将其转发到下一节点，该过程相当于

$Node_{(1)}$→$Node_{(2)}$: *Send*[$E_{NodeKey(2)}$[$\cdots$[$E_{NodeKey(n-1)}$
[$E_{NodeKey(n)}$[*Data*]]]$\cdots$]]];

$Node_{(2)}$→$Node_{(3)}$: *Send* [$E_{NodeKey(3)}$[$\cdots$[$E_{NodeKey(n-1)}$
[$E_{NodeKey(n)}$[*Data*]]]$\cdots$]];

…

$Node_{(n)}$→*Bob*: *Send*[*Data*].

Bob: 目标主机，*NodeKey*(i) ($i=1,2,3,\cdots$): Alice 与第 i 个节点的会话密钥，*Data*: Alice 发往 Bob 的数据.

(2) Bob 发送数据

Bob→$Node_{(n)}$: Response [*Reply-Data*];

$Node_{(n)}$→
$Node_{(n-1)}$: Response [$E_{NodeKey(n)}$[*Reply-Data*]];

$Node_{(n-1)}$→$Node_{(n-2)}$:
Response [$E_{NodeKey(n-1)}$[$E_{NodeKey(n)}$[*Reply-Data*]]];

…

$Node_{(1)}$→Alice: Response [$E_{NodeKey(1)}$[$E_{NodeKey(2)}$
[$\cdots$[$E_{NodeKey(n-1)}$[$E_{NodeKey(n)}$[*Reply-Data*]]]$\cdots$]]].

Reply-Data: Bob 发往 Alice 的响应数据.

4.6　追踪机制

当目标机 Bob 发现匿名用户 Alice 有恶意的匿名访问行为时，触发如图 9 所示的追踪机制，Bob 完成完整性度量后，将用 Alice 的访问日志组成追踪消息发给 Dave，向 Dave 提出追踪 Alice 的申请，Dave 首先对 Bob 的可信性进行评估，杜绝恶意目标主机的非法追踪，通过可信性评估后，Dave 将 Bob 的追踪信息连同 Dave 保存的用户信息一起转发给 AMC，AMC 收到访问日志后，基于行为可信度量机制对匿名用户 Alice 的访问行为进行可信性评估获得 Alice 的行为特征值，当 Alice 是恶意的匿名用户，即 Alice 的行为特征值小于系统安全门限值时，AMC 解密 Alice 的注册签名信息，将 Alice 的基本身份信息通过 Dave 发送给 Bob，Dave 记录恶意用户 Alice 的相关信息，若 Bob 提出虚假的匿名追踪请求，则 AMC 会在特定的数据库中记录 Bob 的诬告行为，将拒绝响应诬告行为达到系统上限的目标主机的匿名性追踪请求.

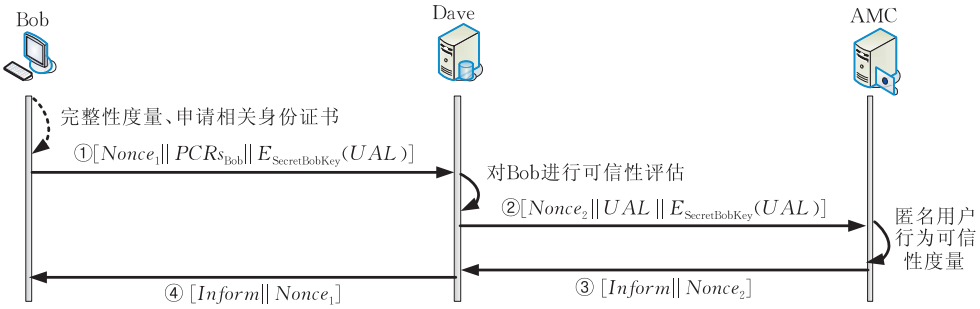


图 9　攻击信息追踪流程

追踪该过程描述如下：

① Bob→Dave：Request[$Nonce_1 \| PCRs_{Bob} \| E_{SecretBobKey}(UAL)$]；

② Dave→AMC：Authentication [$Nonce_2 \| UAL \| E_{SecretBobKey}(UAL)$]；

③ AMC→Dave：AuthResponse [$Inform \| Nonce_2$]；

④ Dave→Bob：Response [$Inform \| Nonce_1$].

UAL：用户 Alice 的访问日志，$Inform$：Alice 的基本注册信息，$Nonce$：随机数用于确认消息是否得到相应的回复.

CTACS 中 AMC 通过行为可信性度量机制获取匿名用户的行为特征值，通过行为特征值与 CTACS 设置的安全门限值间的比较决定是否响应目标主机追踪用户匿名性的请求.

如图 10 所示的行为可信度量机制中，静态可信度量模块主要检测主体访问数据的权限，并将对主体操作的度量信任值提交给控制仲裁；动态度量模块主要提交主体操作结果和操作背景的度量信任值；安全性评估为控制仲裁对主体所有操作行为的可信性评估过程；控制仲裁将动态模块和静态模块对主体行为的度量信任值量化为一个权值，量化的权值即为主体的行为特征值，并在量化过程中控制仲裁加入自身对主体操作的安全性评估值.

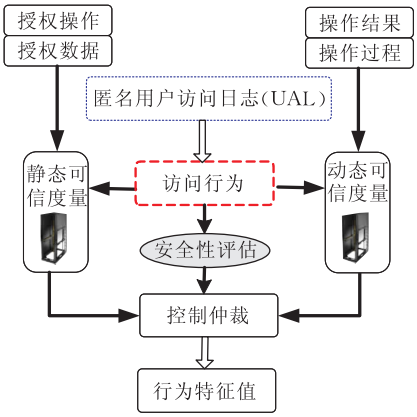


图 10 行为可信的度量机制

AMC 根据 Bob 提交的访问日志，获得 Alice 的度量行为特征值如式(1)所示：

$$Trust(\text{Bob}\rightarrow\text{Alice}):T_1\times\alpha+T_2\times\beta+\left(\frac{\sum_{i=1}^{n}T_{3[i]}}{n}\right)\times\gamma,\quad T_1,T_2,T_{3[i]}\in[0,1] \tag{1}$$

其中，$Trust(\text{Bob}\rightarrow\text{Alice})$表示是 Bob 对 Alice 的访问操作提出质疑时 AMC 对 Alice 的行为进行可信性评估的计算权值；T_1 表示静态度量模块对 Alice 行为的度量信任值；T_2 表示动态度量模块对 Alice 行为的度量信任值；$T_{3[i]}$ 表示控制仲裁对 Alice 第 i 次操作的安全性评估值，n 为 Alice 的访问操作总数，α、β、γ 分别表示百分比，且 $\alpha+\beta+\gamma=1$. CTACS 模型中，当 AMC 经过度量获得的主体行为特征值 $Trust(\text{Bob}\rightarrow\text{Alice})$小于安全门限值 S 时，响应目标主机的匿名性追踪请求，其中 $Trust(\text{Bob}\rightarrow\text{Alice})$、$S\in[0,1]$.

5 CTACS 框架分析

5.1 CTACS 可信匿名接入认证协议分析

节点服务器对申请可控匿名服务的用户通过可信匿名接入认证协议对其进行可信性评估.

5.1.1 协议安全性分析

Bellare 等人在 1998 年引入可证明安全理论模块化的设计思想，后来由 Canetti 等人于 2001 年进一步扩展，称之为通用可组合安全(UC)模型. 本文采用该安全模型来分析、证明 4.2 节中可信匿名接入认证协议的安全性. 相关文献对 UC 模型证明过程所用的通用可组合安全、DDH 假设和多项式时间不可区分性等安全假设进行了详细介绍[19-20].

可信匿名接入认证协议完成 Dave 对 Alice 的身份合法性及平台可信性的验证，其中 $Authentication$ 是 Alice 发往 Dave 的身份合法性及平台可信性验证消息，Dave 通过该消息完成对 Alice 身份合法性及平台可信性的验证. 对于 Dave 而言，只要保证消息 $Authentication$ 确实来自 Alice 且在传输过程中并未被篡改，就可以确保对 Alice 身份合法性及平台可信性验证的正确性，协议中消息认证码和签名机制的使用可以保证 $Authentication$ 消息的上述性质.

为简化协议证明过程，在进行安全性分析证明之前，首先给出可信匿名接入认证协议的抽象描述协议 Π，抽象协议只给出必要的信息. 假设协议在两个实体 I 和 R 间进行，协议 Π 如下所示：

$R\rightarrow I$：$SessionID, Nonce, Secret\text{-}Value, PK_{\text{Alice}}$

$I\rightarrow R$：$SessionID, Nonce, R_{Dave}, PK_{\text{Dave}}$

$R\rightarrow I$：M_1, SIG_1, MAC_1

$I\rightarrow R$：M_2, SIG_2, MAC_2

其中，

$M_1=Nonce_1\|Cert_{\text{AIK}}\|Cert_{\text{Att}}\|R_{\text{Alice}}$；

$M_2=Nonce_1\|Cert_{\text{Alice}}$；

$SIG_1=SIG(R_{\text{Dave}})$；

$MAC_1=\text{Hash}(AliceWriteMacSecret\|M_1)$；

$SIG_2=SIG(R_{\text{Alice}})$；

$MAC_2=\text{Hash}(DaveWriteMacSecret\|M_2)$.

定理 1. 若真实模型下的协议 Π 安全实现了

理想函数 F_{KE}，因此对任何环境机 Z，等式 $REAL_{\Pi,I,Z} \approx IDEAL_{F_{KE},R,Z}$ 均成立，即协议 Π 是 UC 安全的.

证明.　协议 Π 证明思路：首先构造一个能够安全实现签名的理想函数 F_{Sig} 的协议 P_S；其次，给出安全密钥交换的理想函数 F_{KE}，同时构造一个协议 Π_1，并证明 Π_1 在混合模式 F_{Sig}-hybrid 下安全实现了 F_{KE}；将协议 P_S 与 Π_1 进行组合，通过 UC 安全组合定理，证明组合后的协议与 Π 等价，且在现实模型下安全实现了 F_{KE}.　　证毕.

文献[20]详述实现签名的理想函数 F_{Sig} 的协议 P_S 的构造步骤，在此不再赘述.

引理 1.　$Sig=(gen,ID,ver)$ 是文献[19]中描述的签名，那么在真实环境下，协议 P_S 可以安全实现 F_{Sig}，当且仅当 S 是抗击选择消息存在性伪造.

引理 2.　如果 DDH 假设成立，且消息认证算法是安全的，则协议 Π 在 F_{Sig}-hybrid 下安全实现 F_{KE}.

证明.　Π_1 为基于密钥交换理想函数 F_{KE} 的协议，令协议 Π_1 是在混合模型 F_{Sig}-hybrid 下的协议，H 为攻击模型中的攻击者. 构造一个理想环境下的攻击者 S(仿真器)，使得任何环境机 Z 都无法辨别 S 是与 H 及 Π_1 在 F_{Sig}-hybrid 下进行交互，还是与 S 及 F_{KE} 在 Ideal-life 下进行的交互，即对任何环境机 Z，等式 $REAL_{\Pi_1,H,Z} \approx IDEAL_{F_{KE},S,Z}$ 均成立.

使用文献[20]中构造的仿真器 S. 假设在仿真器 S 的执行下，存在一个环境机 Z'，成功辨别与 H 及 Π_1 在 F_{Sig}-hybrid 下进行交互与 S 及 F_{KE} 在 Ideal-life 下进行交互的概率不可忽略，即 $prob(REAL_{\Pi_1},H,Z \neq IDEAL_{F_{KE},S,Z})$ 为 1/2 加上一个不可忽略的优势 ε. 那么使用文献[20]中构造的区分器 D，利用环境机 Z' 来破解 DDH 问题，进而规约到矛盾.

通过对区分器 D 执行过程的分析，并根据区分器的构造原理，得出 D 成功区分输入 Q_0 和 Q_1(Q_0、Q_1 为区分器 D 的输入)的概率等于环境机 Z' 成功辨别理想和混合两种环境的概率，即 D 能够以 1/2 加上一个不可忽略的优势 ε 成功区分 Q_0 和 Q_1，而这与 DDH 假设矛盾，所以得证.　　证毕.

引理 3.　令 Π_1 是 F_{Sig}-hybrid 下的协议，P_S 为安全实现 F_{Sig} 的协议，那么对于任何攻击者 A 都存在一个攻击者 H，使对任何环境机 Z 来说，等式 $REAL_{\Pi P_S,A,Z} \approx IDEAL_{\Pi_1,H,Z}$ 均成立，即组合协议 ΠP_S 安全仿真了 F_{Sig}-hybrid 下的 Π_1.

证明.　根据 DDH 假设即可证明引理 3 成立.

引理 4.　真实环境下，组合协议 $\Pi_1 P_S$ 与协议 Π 等价.

证明.　将混合模型 F_{Sig}-hybrid 下协议 Π_1 对所有理想函数 F_{Sig} 的访问均替换为对协议 P_S 的访问，可以得出协议 $\Pi_1 P_S$ 与协议 Π 等价.

定理 2.　真实模型下的协议 Π 安全实现理想函数 F_{KE}，因此对任何环境机 Z 等式 $REAL_{\Pi,A,Z} \approx IDEAL_{F_{KE},S,Z}$ 均成立，即可信匿名接入认证协议是 UC 安全的.

证明.　根据引理 1～4 及定理 1 即可证得定理 2 成立.

综上所述，可信匿名接入认证协议可安全实现用户与节点服务器间的双向身份认证及可信接入.

5.1.2　协议特点

(1) 高效性. 该协议对通过可信性评估的用户由节点服务器颁发授权接入证书，该证书一次颁发，多次使用，提高工作效率的同时防止节点服务器成为系统瓶颈；

(2) 跨域性. 该协议使用域间匿名认证机制解决 DAA 方案只适用于单信任域的不足，实现验证者和示证者分属不同信任域时平台的真实性验证；

(3) 双向认证. 该协议脱离可信第三方，基于公开密码算法的双向鉴别协议实现用户与节点服务器间的双向身份认证；

(4) 完整性. 该协议中第 2 阶段的通信数据都进行消息认证码校验，保证通信数据不会被篡改，确保通信数据的完整性；

(5) 抗攻击性. 被动攻击仅对通信内容进行截取、窃听和分析等操作，所以安全的密码体制可保证该协议有抵抗被动攻击的能力，协议中随机数及通信双方实体名的使用可以抵抗假冒攻击、重放攻击和中间人攻击等主动攻击方式；

(6) 可控的匿名性. 节点服务器颁发的授权接入证书中不包含用户平台的相关信息，仅报告当前用户平台的身份是否真实、平台的状态是否完整，而没有暴露出平台的基本配置信息，因此有效地保证了用户的隐私性，即授权接入证书具有匿名性，匿名性的强弱来自于有效授权时间的取值，有效授权时间越短则匿名性越强，但授权接入证书的匿名性是可控的，可控性的实现主要依赖于用户的 ID 号，则节点服务器可以确认在证书有效授权时间内完成的接入请求是否来自于同一个用户.

5.1.3　证书间关系

该协议基于证书机制实现用户的安全可信接入，用户持有的各证书间关系如表 1 所示.

表 1 用户证书间的关系

证书名称	作用	颁发条件	颁发者
AIK 证书	平台真实性证明	用户的 TPM 是真实的安全芯片,即通过真实性验证	DAA-Issuer
属性证书	平台完整性证明	平台完整性未遭到破坏,即通过完整性验证	属性证书发布者
授权接入证书	证明用户身份的合法性及平台的可信性	Alice 通过可信性评估,即持有合法的 AIK 证书和属性证书	CTACS 节点服务器

通过对证书的合法性验证,实现节点服务器对用户相关属性的验证,即用户持有合法的 AIK 证书和属性证书是申请授权接入证书的条件.

5.1.4 接入认证机制比较

将本文认证机制与其它各种认证机制就认证效率等特点进行比较,结果如表 2 所示.

表 2 各种认证机制比较

	进行可信评估	可信第三方依赖度	认证效率	是否存在瓶颈	是否支持双向认证
用户密码	否	强依赖	一般	是	否
PKI	否	强依赖	低	是	否
PGP	否	强依赖	一般	是	否
挑战/应答	否	强依赖	一般	是	否
IC 卡	否	强依赖	一般	是	否
指纹识别	否	强依赖	一般	是	否
本文协议	是	无第三方	高	否	是

5.2 CTACS 安全性分析

CTACS 模型的安全性体现在以下 5 个方面:

(1) CTACS 节点信息集中管理. 节点服务器上保存所有 CTACS 节点的信息,节点服务器可以定时对 CTACS 的所有节点进行可信度量,一旦发现某个节点处于不可信状态,将该节点信息从相应的数据库中删除,则将该节点就从 CTACS 中删除,CTACS 节点集中管理机制便于 CTACS 随时发现系统中不安全的节点,并将其从系统中删除,进而确保 CTACS 的安全性和可信性.

(2) TPM 安全芯片的核心作用. 方案突出了 TPM 在 CTACS 框架中的功能,无论是以 TPM 唯一硬件标识信息为主的身份认证过程,还是基于 TPM 实现的系统安全启动和完整性度量过程,TPM 均在其中发挥了重要的作用,TPM 是 CTACS 模型中实现身份认证和信任链传递的硬件基础.

(3) 完整的信任链传递. 在 CTACS 框架中,以 TPM 安全芯片和安全 BIOS 为信任源,建立一个完整的从 BIOS 加载、操作系统加载直至 CTACS 的信任链传递模型,将信任关系由终端传递到匿名通信系统中.

(4) 节点的接入度量. CTACS 的匿名通信链路建立时,首先对准备接入链路的 CTACS 节点进行可信性评估,只有当该节点处于可信状态时,才将其接入链路,节点的接入度量机制进一步确保了 CTACS 的安全性,防止某些节点在服务器度量后成为不安全节点,而用户却误将其接入链路.

(5) 数据的加密传输. 用户主机将信息数据加密后通过 CTACS 发出,加密过程是将数据以及目标地址和源地址等包头信息都按途经 CTACS 节点的先后顺序使用相应的对称密钥将其层层加密,每经过一个 CTACS 节点解密一次,直到目标主机时才将所有的加密处理完. 同时采用加密传输的方式发送数据,可以有效地阻止公网上的窃听和流量分析等攻击行为,提供双向、实时的匿名连接. 若在链路建立后,链路中的某个节点被黑客所控制,由于每个节点只知道自己的加/解密密钥,则该黑客只能从数据包中得知该节点的直接前驱和直接后继的位置,根本无法获知数据真正的源地址和目标地址,除非黑客控制该链路中所有的节点,而这在现实中是很难实现,因此 CTACS 模型,很好地保护了用户信息的安全性.

5.3 CTACS 可信性分析

用户在接入 CTACS 时,首先进行基于 TPM 的完整性度量,AMC 和节点服务器对其完整性度量信息进行可信性评估,只有通过评估的用户才允许接入 CTACS,用户接入时的可信性评估操作确保接入 CTACS 用户的可信性;同时 CTACS 中的所有节点定期根据 Dave 的要求随时进行完整性度量操作,并将度量结果报告给节点服务器,由其对节点的度量信息进行评估,根据评估结果,将不再可信的系统节点移出 CTACS,节点定期的可信性评估操作确保构建 CTACS 节点的可信性;若用户出现恶意行为时,通过 AMC 对其身份信息的追踪,使得目标机可以获知恶意行为用户的真实信息,CTACS 的追踪机制确保了用户行为的可信性.

在 CTACS 中,建立以 TPM 为核心的信任链传递过程和可信度量过程,以及节点接入时的可信性评估机制,确保接入 CTACS 用户的可信性以及构建 CTACS 节点的可信性,由用户以及链路节点的可信进而保证 CTACS 是可信的通信系统.

5.4 CTACS 匿名性分析

使用 CTACS 模型框架时,用户首先启动相应的代理程序,从 CTACS 节点服务器上随机地下载一定数量的节点信息并建立匿名链路,由于每次随机所选择的节点各不相同,建立的链路就不相同,因

此攻击者无法通过 CTACS 的链路进行匿名性攻击. 当用户使用 CTACS 上网时，首先建立一条通信链路，由于链路的转发数据是经过用户代理程序层层加密处理的，而链路中的转发节点仅知道自己的加/解密密钥，所以转发节点仅知道自己的直接前驱和直接后继，不可能知道路径中的其它节点，外部观察者即使侦听到通信数据，而他们所看到的 IP 数据报中的地址并不是通信发起者和接收者的真实地址，因此用户的真实身份和目标地址都被隐藏，进而隐藏了用户的网络行为，所以说 CTACS 具有匿名性，即 CTACS 满足用户的匿名性需求.

5.4.1　匿名的可控性分析

在 CTACS 模型中，当目标主机发现用户有恶意的匿名行为时，目标主机将向节点服务器发出追踪用户匿名性的请求，节点服务器首先对目标主机的真实性进行验证，防止恶意目标主机追踪行为的发生，对通过可信性评估的匿名性追踪请求，节点服务器将追踪信息连同服务器所保存的签名信息一起发送给 AMC，AMC 基于行为可信性度量机制获得匿名用户的行为特征值，恶意用户的行为特征值必定小于 CTACS 设置的安全门限值，AMC 解密恶意用户注册时的签名信息，将用户的基本身份信息通过节点服务器发送给目标主机，目标主机获得恶意用户的真实身份后，对其进行一些必要的控制操作，如限制其操作权限或拒绝服务请求. 行为可信性度量机制、群签名技术和追踪机制的运用确保 CTACS 是可控的匿名通信系统.

本文对 CTACS 追踪机制中行为可信度量机制中决策式(1) $Trust$(Bob→Alice)的变化过程进行仿真，并对仿真结果进行分析.

图 11 所示为 $Trust$(Bob→Alice)在不同 α、β、γ 的比例分配下的变化曲线. 设在正常情况下，静态模块的度量信任值为 0.8，动态模块的度量信任值为 0.65，行为的安全性评估信任值为 0.6. 图 11 中的黑色区域即为 $Trust$(Bob→Alice)在不同分配比例下的变化曲线图. 当 $\alpha=1$ 时，$Trust$(Bob→Alice)取得最大值 0.8；当 $\gamma=1$ 时，$Trust$(Bob→Alice)取得最小值 0.6，所以目标主机可以根据侧重点的不同，动态地调节 α、β、γ 的比例分配，根据 $Trust$(Bob→Alice)的变化情况来选取合适的控制门限值 S.

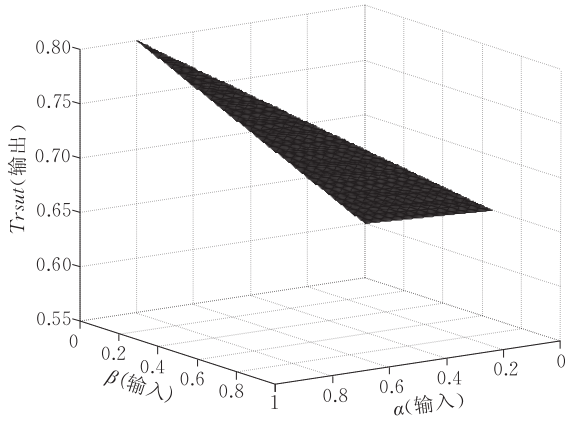


图 11　可信度量机制在不同参数下的变化图

图 12 所示为 $Trust$(Bob→Alice)在追踪触发过程中的变化曲线，其中，$\alpha=0.45$，$\beta=0.15$，$\gamma=0.4$，行为的安全性评估信任值为 0.3，图 12 中的黑色区域即为该状态下 $Trust$(Bob→Alice)的取值变化范围. 随着主体行为静态模块和动态模块可信评估值的增加，在主体行为完全可信时，$Trust$(Bob→Alice)可以达到的最大值为 0.72.

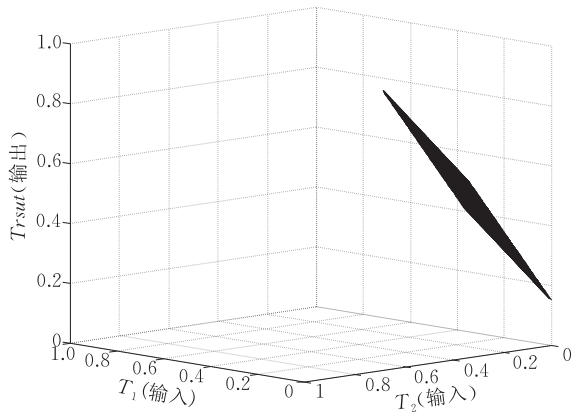


图 12　可信度量机制在交互过程中的变化图

5.4.2　匿名的抗攻击性分析

文献[21]由易到难定义了 8 种攻击方式，针对这些攻击方式，本文对 CTACS 匿名的抗攻击能力进行分析，分析表明 CTACS 对文献[21]定义的 8 种攻击方式均能抵抗，分析结果如表 3 所示.

表 3　CTACS 抗攻击性分析

攻击类型	抗攻击性分析
消息码攻击	抵抗，用公钥加密对通信双方(源主机和目标主机)进行保护.
消息长度攻击	在各节点间进行保护，终端处未保护.
重放攻击	抵抗，通过时间戳、随机数等机制实现抵抗.
合谋攻击	抵抗，仅当链路的 N 个节点中有 $N-1$ 个串通时才会被攻破.
泛洪攻击	抵抗，节点服务器对用户平台的可信性评估可以抵抗泛洪攻击.
消息量攻击	抵抗，填充机制使消息长度在各节点间传输时不变，填充机制可以抵抗消息量攻击.
时间攻击	在各节点间提供保护，终端处未保护.
侧面攻击	抵抗，层层加密机制可以抵抗流量分析、窃听等攻击行为.

5.4.3 技术对比

本文将 CTACS 和 Tor 匿名通信系统在接入策略等方面进行比较,详见表 4 所示.

表 4 CTACS 与 Tor 匿名通信系统的对比

对比项	CTACS	Tor 匿名通信系统
节点服务器的保护措施	基于可信计算的安全防护+传统的安全措施,安全等级高	仅有传统的安全措施:防火墙+杀毒软件+入侵检测
节点服务器的接入策略	身份认证+基于可信计算的平台可信性评估	仅有身份认证
节点的接入控制策略	可信性评估	无
节点的安全性保障	定时评估节点的可信性,提高系统的可靠性与安全性	无
匿名的抗攻击性	对文献[21]中定义的 8 种攻击类型均能抵抗,抗攻击能力强	只能抵抗文献[21]中定义的部分攻击,抗攻击能力适中
匿名的可控性	提供可控的匿名服务	无可控性

分析表明 CTACS 较 Tor 匿名通信系统而言,在具有可控性和可信性的同时,具有更高的安全性及抗攻击能力,可由相关可信组织(如政府机构、中国可信计算工作组、TCG等)提供节点服务器、身份认证中心及几个固定的节点组成 CTACS 框架的雏形,当用户使用 CTACS 时,其首先加入 CTACS 作为成员节点,将其完整性度量信息及其它一些必要信息保存到服务器上,该方案随着系统用户人数的增加,匿名效果会更好,同时网络的运行速度更快、用户信息的匿名性更高、模型更加安全、可信.

5.5 CTACS 效率分析

CTACS 方案在 TPM 安全芯片、时间和空间上都达到较高的效率.

TPM 利用率. 在可控可信匿名链路建立过程中,对每个 CTACS 节点首先基于 TPM 进行完整性度量,只有当该节点的度量摘要与服务器上的度量信息相匹配时,才将该节点接入 CTACS,同时服务器定期会对所有 CTACS 节点的可信性进行度量,对节点的可信度量机制在一定程度上提高了 TPM 安全芯片的利用效率.

时间效率. 该框架中用各 CTACS 节点基于 TPM 的可信度量代替传统的计算各节点间信任值的方式来建立可信链接,度量过程与信任值的计算相比较节约时间.

空间效率. 该框架中只有服务器需要一定数量的存储空间用来存放 CTACS 的所有节点的相关信息,而其它节点不需要空间来存放,大大减少了用户存储空间的占用量.

工作效率. 该框架中证书机制的应用,降低了节点服务器的工作强度和用户及节点的完整性度量负载,同时防止节点服务器成为系统瓶颈,提高了整个 CTACS 的工作效率.

6 结束语

本文基于可信计算技术提出一种可控可信的匿名通信方案,该方案在一定程度上解决了当前在可控匿名技术及可控匿名系统研究的不足,同时较好地将匿名通信与可信计算技术进行融合,提高了节点服务器的安全性. 通过对接入系统的节点进行可信性验证,在增强整个系统的安全性、消除用户匿名通信过程的安全隐患、为服务方提供可追踪匿名服务的同时确保了本匿名方案具有更好的可控性、可信性与安全性. 授权接入证书的应用,提高了系统的工作效率,防止节点服务器成为 CTACS 的瓶颈. 下一步的研究方向是建立 CTACS 信任链模型,并进行相关原型的实现.

参 考 文 献

[1] Claessens J, Diaz C, Goemans C. Revocable anonymous access to the internet. Internet Research: Electronic Networking Application and Policy, 2003, 13(4): 242-258

[2] Yang Tian-Xiang. International comparative analysis of the right to web privacy protection. Journal of Shanghai Business School, 2007, 8(4): 41-44(in Chinese)
(杨天翔. 网络隐私权保护:国际比较分析与借鉴. 上海商学院学报, 2007, 8(4): 41-44)

[3] Diaz Claudia. Anonymity and privacy in electronic services [Ph. D. dissertation]. Katholieke Universiteit Leuven, Leuven, Belgium, 2005

[4] Stefan K, Rolf W Hannes. Revocable anonymity//Proceedings of ETRICS 2006. Freiburg, Germany, 2006. LNCS 3995. Springer-Verlag, Heidelberg, 2006: 206-220

[5] Claessens J, Diaz C, Goemans C et al. Revocable anonymous access to the Internet. Journal of Internet Research, 2003, 13(4): 242-258

[6] Lin Chuang, Lei Lei. Research on next generation Internet architecture. Chinese Journal of Computers, 2007, 30(5): 694-711(in Chinese)
(林闯, 雷蕾. 下一代互联网体系结构研究. 计算机学报, 2007, 30(5): 694-711)

[7] Zhang Hong-Ke, Su Wei. Fundamental research on the architecture of new network—Universal network and pervasive services. Acta Electronica Sinica, 2007, 35(4): 593-598(in Chinese)

(张宏科，苏伟. 新网络体系基础研究——一体化网络与普适服务. 电子学报，2007，35(4)：593-598)

[8] Luo Jun-Zhou，Han Zhi-Geng，Wang Liang-Min. Trustworthy and controllable network architecture and protocol framework. Chinese Journal of Computers，2009，32(3)：391-404 (in Chinese)
(罗军舟，韩志耕，王良民. 一种可信可控的网络体系及协议结构. 计算机学报，2009，32(3)：391-404)

[9] Dai Jiang-Shan，Xiao Jun-Mo. Method of tracing attacks based on controllable network. Journal of Nanjing University of Science and Technology，2005，29(3)：356-359(in Chinese)
(戴江山，肖军模. 一种基于可控网络的攻击源定位方法. 南京理工大学学报，2005，29(3)：356-359)

[10] Zhou Yan-Wei，Wu Zhen-Qiang et al. Study of new trusted network framework. Journal of Computer Applications，2009，29(9)：2355-2359，2365(in Chinese)
(周彦伟，吴振强等. 新的可信网络框架研究. 计算机应用，2009，29 (9)：2355-2359，2365)

[11] Greenberg A，Hjalmtysson G，Maltz D A et al. A clean slate 4D approach to network control and management. ACM SIGCOMM Computer Communication Review，2005，35(5)：41-54

[12] Chen Xin，Hu Hua-Ping，Liu Bo et al. Hierarchical location-diversity-based low-delay anonymous communication framework. Journal on Communications，2009，30(5)：54-61(in Chinese)
(陈新，胡华平，刘波等. 分层基于地理多样性的低延迟匿名通信架构. 通信学报，2009，30(5)：54-61)

[13] Wu Zhen-Qiang，Ma Jian-Feng. A joint-entropy-based anonymity metrics model with multi-property. Journal of Computer Research and Development，2006，43(7)：1240-1245 (in Chinese)
(吴振强，马建峰. 基于联合熵的多属性匿名度量模型. 计算机研究与发展. 2006，43(7)：1240-1245)

[14] Wu Zhen-Qiang，Ma Jian-Feng. A dynamic mix anonymity algorithm for wireless Ad Hoc networks. Journal of Computer Research and Development，2007，44(4)：560-566 (in Chinese)
(吴振强，马建峰. 一种无线 Ad Hoc 网络动态混淆匿名算法. 计算机研究与发展，2007，44(4)：560-566)

[15] Sui Hong-Fei，Chen Song-Qiao，Chen Jian-Er et al. Payload analysis of rerouting-based anonymous communication systems. Journal of Software，2004，15(2)：278-285 (in Chinese)
(眭鸿飞，陈松乔，陈建二等. 基于重路由匿名通信系统的负载分析. 软件学报，2004，15(2)：278-285)

[16] Aaron Johnson，Paul Syverson. More anonymous onion routing through trust//Proceedings of the 22nd IEEE Computer Security Foundations Symposium (CSF 2009). Port Jefferson，New York，2009：3-12

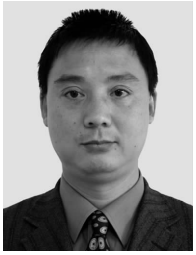
[17] Berthold O，Pfitzmann A，Standtke R. The disadvantages of free MIX routes and how to overcome them//Federrath H ed. Proceedings of the Designing Privacy Enhancing Technologies：Workshop on Design Issues in Anonymity and Unobservability. LNCS 2009. Springer-Verlag，2000：30-45

[18] Li Jie，Wu Zhen-Qiang et al. An improved directed anonymous attestation scheme. Journal of Computer Applications，2009，29(2)：364-366，397(in Chinese)
(李洁，吴振强等. 一种改进的直接匿名认证方案. 计算机应用，2009，29(2)：364-366，397)

[19] Goldwasser S，Micali S，Rivest R. A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal on Computing，1998，17(2)：281-308

[20] Cao Chun-Jie，Yang Chao，Ma Jian-Feng，Zhu Jian-Ming. An authentication protocol for station roaming in WLAN Mesh. Journal of Computer Research and Development，2009，46(7)：1102-1108(in Chinese)
(曹春杰，杨超，马建峰，朱建明. WLAN Mesh 漫游接入认证协议. 计算机研究与发展，2009，46(7)：1102-1108)

[21] Wu Zhen-Qiang. Anonymous communications for attack-resistant. Journal of Shaanxi Normal University (Natural Science Edition)，2004，32(1)：29-32(in Chinese)
(吴振强. 匿名技术的抗攻击性研究. 陕西师范大学学报(自然科学版)，2004，32(1)：29-32)



WU Zhen-Qiang，born in 1968，Ph. D.，associate professor. His research interests include anonymous communication，trusted computing，adaptive security architecture and wireless network security.

ZHOU Yan-Wei，born in 1986，M. S.. His research interests include anonymous communication and trusted computing.

QIAO Zi-Rui，born in 1985，M. S.. Her research interests focus on intelligent information processing.

Background

This work is supported by the National Natural Science Foundation of China (60633020) and the National High Technology Research and Development Program (863 Program) of China (2007AA01Z438200).

Anonymity and identity management technologies are powerful tools to protect privacy. Nevertheless, their potential for abuse is a factor that hinders the development and implementation of privacy enhancing systems at a large scale. The past two decades have seen a growing interest in methods for anonymous communication on the Internet, both from the academic community and the general public. Several system designs have been proposed in the literature, of which a number have been implemented and are used by diverse groups, such as journalists, human rights workers, the military, and ordinary citizens, to protect their identities on the Internet.

This paper discusses the requirements of a controllable and trusted anonymous communication that a large scale anonymity infrastructure should comply with in order to be acceptable for all parties. The authors survey the Trusted Computing Platform that is the industrial initiative to implement computer security. However, privacy protection is a critical problem that must be solved in Trusted Computing Platform. Two solutions have been proposed in the specification of TPM. TPM v1.1 is based on a trusted third party, called Privacy CA. Obviously, this is not satisfactory solution, since each transaction needs the involvement of Privacy CA, and the compromise of CA will disclose all mapping between AIK's and EK. The solution in TPM v1.2 is called direct anonymous attestation (DAA) in which TPM can directly proves its authenticity to a remote server with the help of Privacy CA. But so far this specification would not hide a sender's (or recipient's) network address (IP address, email address, etc.) on the Internet anonymous communication system.

This paper presents a controllable and trusted anonymous communication architecure that consists of four functional modules, like authentication management center (AMC), trusted user node list that was downloaded from the server, established anonymous communication link, and traceable service of malicious behavior. The paper has carried on the systematization design to these modules, and has given each module a corresponding protocol. The architecture can meet the demand of the large scale deployment of anonymous communication system in the future Internet.