doi:10.11959/j.issn.1000-436x.2015138

多样化的可控匿名通信系统

周彦伟，吴振强，杨波
（陕西师范大学 计算机科学学院，陕西 西安 710062）

摘 要：随着网络通信技术的发展，Tor 匿名通信系统在得到广泛应用的同时暴露出匿名性较弱等不安全因素，针对上述问题，基于节点的区域管理策略提出一种多样化的可控匿名通信系统(DC-ACS)，DC-ACS 中多样化匿名链路建立机制根据用户需求选择相应区域的节点完成匿名通信链路的建立，同时基于行为信任的监控机制实现对用户恶意匿名行为的控制，并且保证了发送者和接收者对匿名链路入口节点和出口节点的匿名性。通过与 Tor 匿名通信系统的比较，DC-ACS 在具有匿名性的同时，具有更高的安全性和抗攻击的能力，解决了 Tor 匿名通信系统所存在的安全隐患。

关键词：匿名通信系统；Tor；信任评估；多样性
中图分类号：TP393.08 **文献标识码**：A

Diversity of controllable anonymous communication system

ZHOU Yan-wei, WU Zhen-qiang, YANG Bo
(School of Computer Science, Shaanxi Normal University, Xi ' an 710062, China)

Abstract: With the development of network communication technology, the Tor anonymous communication system has been widely used. However, there are also some unsafe factors such as insufficient anonymity which deserves to be noticed. Thus, a diversified controllable anonymous communication system (DC-ACS) was proposed based on the node regional management strategy. The diversified anonymous link establishment mechanism chooses nodes in the corresponding field to build the anonymous communication link according to users' needs, controls users' malicious anonymous activities, and ensures the anonymity of senders and receivers to the first and last node of anonymous communication link. Compared with the Tor anonymous communication system, DC-ACS not only has anonymity, but also has higher security and anti-attack capability, which eliminated potential security risks existed in the Tor anonymous communications system.

Key words: anonymous communication system; Tor; credible appraisal; diversity

1 引言

Internet 作为通信与信息传播的工具处于快速发展并且广为人们所接受，与此同时安全与隐私逐步成为 Internet 的一个关键问题。文献[1]中的民意测验表明用户使用 Internet 时感到最大的障碍就是担心自己的隐私被发现。匿名通信即在不改变现有网络协议的前提下实现业务流中通信关系的隐藏，完成对用户身份等隐私信息的保护，使窃听者无法直接获知或间接推知双方的通信关系或身份[2]。

针对用户的匿名性需求，目前已有很多的匿名通信系统，如 Anonymizer[3]、Onion Routing[4]、Tor[5,6]、Crowds[7]、Tarzan[8]、Mixminion[9]、Sherwood[10]、DC-Net[11]和 WonGoo[12]等。其中，Tor

收稿日期：2014-06-24；**修回日期**：2014-09-09
基金项目：国家自然科学基金资助项目(61272436, 61402275)；陕西省自然科学基金资助项目(2014JQ8309)；保密通信重点实验室基金资助项目(9140C110206140C11050)；中国科学院信息工程研究所信息安全国家重点实验室开放课题基金资助项目(2015-MS-10)；中央高校基本科研业务费专项基金资助项目(GK201504016, GK20130205)
Foundation Items: The National Natural Science Foundation of China (61272436, 61402275);The National Natural Science Foundation of Shaanxi Province (2014JQ8309); The Foundation of Science and Technology on Communication Security Laboratory (9140C110206140C11050); The Foundation of State Key Laboratory of Information Security (2015-MS-10); The Fundamental Research Funds for the Central Universities (GK201504016, GK20130205)

匿名通信系统因配置简单、性能优良得到迅速发展及广泛应用，Tor 不仅可抵抗侦听和流量分析等攻击，还具有前向安全、拥塞控制、可变出口策略及端到端的完整性检测等特点，是目前互联网上应用最广泛的匿名通信系统之一，然而随着 Internet 技术的发展及匿名通信原理的深入研究，发现 Tor 在用户体验、匿名链路建立过程存在一些不足，影响了 Tor 匿名通信系统的推广应用及发展[13]。

本文提出多样化的可控匿名通信系统(下文简称为 DC-ACS)，DC-ACS 在确保用户匿名通信的基础上，具有更高的安全性和匿名性，为用户提供更加安全可靠的匿名通信服务，弥补了传统 Tor 匿名通信系统所存在的不足。

2 相关工作介绍

Tor 匿名通信系统为用户建立一条到达目标主机的匿名通信链路，匿名链路的中继节点仅知道自己的直接前驱和直接后继，但是无法获知路径中其他节点的地址信息，外部观察者即使检测到通信数据，而其所能识别的地址信息并非发起者和接收者的真实地址[13,14]。研究发现 Tor 匿名通信系统在用户体验、匿名链路建立等方面存在下述不足。

1) 用户选择的灵活性不够

由于匿名链路基于固定算法建立，导致用户无法自主控制链路的匿名性和传输效率，然而在实际应用中，不同的应用数据对链路的匿名性和传输效率的要求并不相同；例如普通网站和电子商务网站对浏览匿名性的要求就不同，网站浏览和即时通信对通信效率的要求就不相同，即有的应用更关注链路的匿名性，而有的应用却更关注链路的通信效率。

2) 密钥协商过程易受中间人攻击

匿名链路建立时，用户与各中继节点间基于 Differ-Hellman 密钥协商协议完成会话密钥的协商，由于 Differ-Hellman 密钥协商协议易受中间人攻击，导致 Tor 密钥协商过程同样易受中间人攻击。

3) 未达到最佳的匿名效果

虽然 Tor 较好地满足了用户的通信匿名需求，由于匿名链路的中继节点能够准确定位前驱节点和后继节点，使入口节点掌握发送者的地址等隐私信息，出口节点掌握接收者的地址等隐私信息，即发送者和接收者的匿名性存在不足。

4) 缺乏恶意匿名用户的控制机制

由于 Tor 匿名通信系统具有较强的匿名性，有效保护了用户的私密性，由于 Tor 对匿名用户的操作缺乏监督机制，导致 Tor 在保护合法用户隐私的同时，同样隐藏了攻击者的恶意访问行为。

为解决 Tor 匿名系统所存在的不足，本文提出了多样化的可控匿名通信系统，该系统中用户基于节点的分区管理策略按需建立匿名通信链路，其中匿名链路的首尾节点无法获知发送者和接收者的具体信息；基于行为可信性的监控机制实现对恶意匿名行为的可控性。

3 多样化可控匿名通信系统

针对传统 Tor 匿名通信系统在用户体验和链路构建过程中所存在的不足，本文提出多样化可控的匿名通信系统。如图 1 所示，Alice 为匿名用户；Bob 为网络服务提供商；Dave 为目录服务器，基于

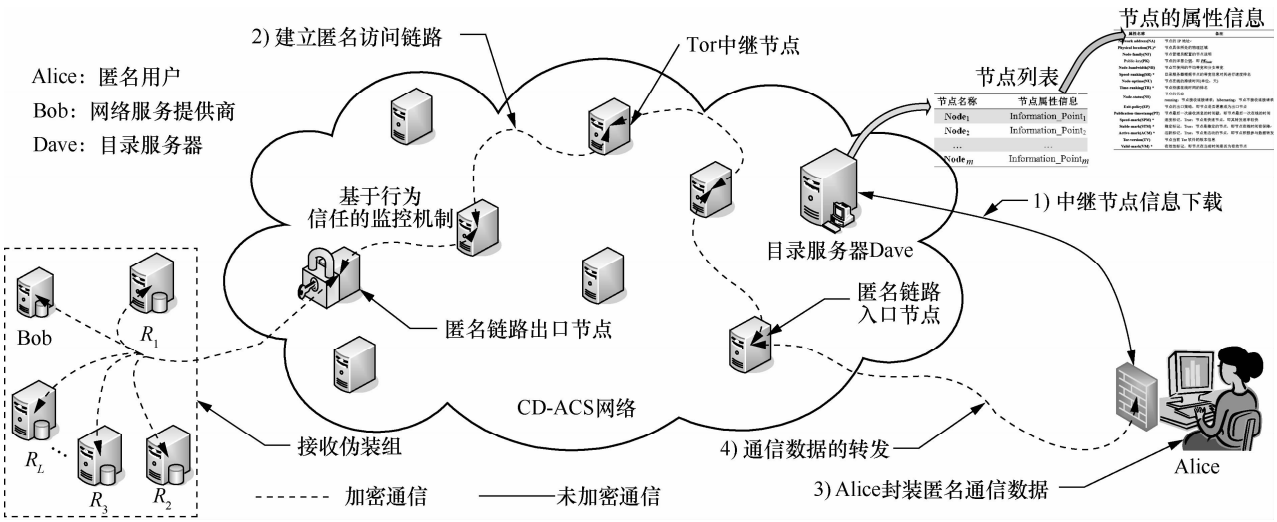

图 1 可控的多样性 Tor 匿名通信系统

相关可信性验证策略[15,16]对中继节点进行平台可信性验证，并根据验证结果更新节点列表，确保中继节点的身份合法性及平台可信性。

DC-ACS 的具体工作步骤如下所述。

1) 节点的按需下载

Alice 根据应用数据对匿名性及传输性能的要求，从 Dave 下载满足要求的中继节点信息。下载过程中，Dave 基于可信匿名接入认证协议[17]完成对 Alice 的身份合法性及平台可信性验证。

2) 匿名链路的建立

Alice 启动本机上的链路建立程序与中继节点及 Bob 间协商共享的会话密钥，建立一条安全的匿名通信链路。

3) 匿名通信数据的封装

Alice 运用消息封装算法生成匿名通信数据，即根据匿名链路中各中继节点从后至前的顺序对通信消息依次进行嵌套加密封装，并将 Bob 隐藏在由同区域主机构成的接收伪装组中，同时 Alice 对匿名通信数据的源地址进行编码处理。

4) 匿名通信数据的转发

Alice 通过匿名通信链路发送封装后的匿名通信消息，匿名链路中各中继节点基于消息转发策略对其进行转发，直至 Bob 匿名数据才被完全解密。

本文中相关变量及运算的定义如表 1 所示。

表 1　　变量及运算的定义

符号	定义
n	大素数
r_A	A 选取的随机秘密数
L	接收伪装组的成员数
D_A	A 的共享密钥协商信息
(KS_A, KP_A)	A 的公私钥对
KS_A^{-1}	关于 A 私钥 KS_A 的求逆运算值，且满足 $KS_A^{-1}KP_A= P$，P 为常数
$K_{(A, B)}$	A 与 B 协商的会话密钥
$H()$	标准单向散列函数
$E(k, m)/D(k, c)$	对称密钥加密/解密算法
$IP\_XOR(IP_1, IP_2)$	IP 地址的异或运算函数，返回值仍为标准的 IP 地址

3.1　节点管理机制

Tor 匿名通信系统中目录服务器存储了节点的 IP 地址、洋葱公钥、出口策略、带宽和在线时长等信息。为实现对其不足的改进，本文对目录服务器中节点的属性信息进行扩充，以满足用户的多样性匿名需求。扩展属性均可根据已有属性进行初始化，属性的扩展方便了用户下载过程中节点的选择，但并未增加目录服务器管理的复杂性；同时目录服务器定期对节点的身份合法性及平台可信性基于相关策略进行验证，文献[16,18,19]对平台的可信性验证策略及关键技术进行了介绍及研究。

3.1.1　节点属性

根据实际应用，本文在原有节点属性的基础之上，增加相关状态的标记属性。扩展后的属性信息如表 2 所示。

表 2　　扩展后的中继节点属性信息

属性名称	备注
network address(NA)	节点的 IP 地址
physical location(PL)*	节点具体所处的物理区域
node-family(NF)	节点管理员配置的节点说明
public-key(PK)	节点的洋葱公钥，即 PK_{Node}
node-bandwidth(NB)	节点可使用的平均带宽和分支带宽
speed-ranking(SR) *	节点的带宽排序
node-uptime(NU)	节点在线的持续时间/天
time-ranking(TR) *	节点持续在线时长的排序
node-status(NS)	节点的状态 running：节点接收连接请求；hibernating：节点不接收连接请求
exit-policy(EP)	出口策略，表示节点是否愿意成为出口节点
publication-timestamp (PT)	节点最后一次接收消息的时间戳，即节点最后一次在线的时间
speed-mark(SPM) *	速度标记，True 表示快速节点
stable-mark(STM) *	稳定性标记，True 表示稳定节点
active-mark(ACM) *	活跃性标记，True 表示活跃节点
Tor-version(TV)	节点当前 Tor 软件的版本信息
valid-mark(VM) *	有效性标记，即节点在当前时间是否有效

注：带*的为本文扩充属性

3.1.2　节点管理策略

目录服务器根据算法 1 所示的管理策略定期对所有中继节点进行管理，并更新相应的属性。

算法 1　节点管理策略

Begin

① Ini_Function(Node)；

//初始化节点属性，根据 IP 地址初始化 PL 属性；根据带宽大小和持续在线时长对各节点排序，即初始化 SR 和 TR 属性；

② **IF**(Node.TV==不存在故障的 Tor 软件版本)

　　Node.VM=True；//节点在当前时间有效

　Else

　　Node.VM=False；

End IF //初始化节点的状态信息

③ **IF**(|Time-Node.PT|<10 (house) && Node.NS == running && Node.VM == True)

Node.ACM=True；//下线时间不超过 10 h；且状态为 running 的有效节点是活跃节点。

Else

Node.ACM=False；

End IF //初始化节点的活跃性状态

④ **IF** (Node.NU>30 || Node.TR<20)

Node.STM=True；//持续时间在 30 天以上或在线时间排名前 20 名的节点都是稳定节点。

Else

Node.STM=False；

End IF //初始化节点的稳定性状态

⑤ **IF** (Node.NB>100 kB/s || Node.SR<20)

Node.SPM=True；//带宽在 100 kB/s 以上或带宽处于前 20 位的节点都是快速节点。

Else

Node.SPM=False；

End IF //初始化节点的速度状态

⑥ 对节点的合法性及平台可信性基于相关策略进行验证；

End //算法中的相关参数由目录服务器设置；为方便算法说明，本文选取的参数较小。

3.2 节点下载算法

根据节点属性的扩充，本文提出如算法 2 所示的中继节点下载算法，根据用户需求下载相关中继节点的信息，给予用户平衡传输链路匿名性和传输效率的能力，对于匿名性要求高的数据建立匿名性强的匿名链路，对于时效性要求高的数据建立传输效率高的匿名链路，即用户在匿名链路建立过程中具有较强的自主性。

匿名链路属性包括：性能优先(PS, performance service)和匿名性优先(AS, anonymity service)。PS 表示用户更加关注匿名链路传输的性能，需要匿名链路提供相对更优的传输效率；AS 表示用户更加关注匿名链路传输的匿名性，需要匿名链路提供相对更优的匿名性。

算法 2 节点下载算法

Begin

IF (Alice.Link_Attribute==PS)

For i=1to n //n 为匿名链路的长度

IF(Node$_{(i)}$.PL==Alice.PL&& Node$_{(i)}$.SPM==True && Node$_{(i)}$.ACM==True)

选择该节点，并下载相关信息；

End IF

End For //选择相同区域活跃的快速节点建立性能优先的匿名链路

Else

IF(Alice.Link_Attribute==AS)

For i=1to n

IF(Node$_{(i)}$.PL!=Alice.PL&& Node$_{(i)}$.SPM==True && Node$_{(i)}$.STM==True)

选择该节点，并下载相关信息；

End IF

End For //选择不同区域稳定的快速节点建立匿名优先的匿名链路

Else //表示用户对传输链路的匿名性和传输效率不做任何要求

For i=1to n

IF (Node$_{(i)}$.VM==True)

选择该节点，并下载相关信息；

End IF//选择有效节点建立匿名链路

End For//传统 Tor 匿名通信系统使用该方法建立匿名链路

End IF

End IF

End

3.3 匿名链路建立

Alice 根据需求从 Dave 下载一定数量的中继节点，建立到达目标主机 Bob 的匿名通信链路，具体的共享密钥协商及匿名链路建立过程如下。

Alice 选取随机秘密数 $r_1 \in [2, n-1]$，并计算 $D_1 = (r_1 + KS_A)KP_X$，然后发送 Create 命令给匿名链路的首节点 X，Create 命令的负载为使用 X 的洋葱公钥加密的密钥协商信息 D_1；X 收到 Create 命令后，使用洋葱私钥解密数据得到 D_1，选取随机秘密数 $r_X \in [2, n-1]$，计算 $D_X = (r_X + KS_X)KP_A$，X 计算与 Alice 间的会话密钥 $K_{(A,X)} = KS_X^{-1}(r_X + KS_X)D_1$；然后发送 Created 命令给 Alice，Created 命令包含密钥协商信息 D_X 和会话密钥 $K_{(A,X)}$ 的散列值 $H(K_{(A,X)})$。Alice 收到 Created 命令后，Alice 计算与 X 间的会话密钥 $K_{(A,X)} = KS_A^{-1}(r_1 + KS_A)D_X$。此时，Alice 与 X 间的匿名链路建立完成，同时 Alice 与 X 完成会话密钥的协商，并且基于会话密钥的散列值完成对密钥协商过程的完整性验证。

Alice 计算的会话密钥为

$$K_{(\mathrm{A,X})}=KS_{\mathrm{A}}^{-1}(r_{\mathrm{I}}+KS_{\mathrm{A}})D_{\mathrm{X}}=(r_{\mathrm{I}}+KS_{\mathrm{A}})(r_{\mathrm{X}}+KS_{\mathrm{X}})P$$

节点 X 计算的会话密钥为

$$K_{(\mathrm{A,X})}=KS_{\mathrm{X}}^{-1}(r_{\mathrm{X}}+KS_{\mathrm{X}})D_{\mathrm{I}}=(r_{\mathrm{I}}+KS_{\mathrm{A}})(r_{\mathrm{X}}+KS_{\mathrm{X}})P$$

Alice 选取随机秘密数 $r_2\in[2,n-1]$，并计算 $D_2=(r_2+KS_{\mathrm{A}})KP_{\mathrm{Y}}$，然后发送 Extend 命令给匿名链路的首节点 X，负载包含中继节点 Y 的地址和使用 Y 的洋葱公钥加密的密钥协商信息 D_2；X 接收到 Extend 命令后，创建对应的 Create 命令并传输消息 $E\{KP_{\mathrm{Y}},D_2\}$给 Y；当 Y 收到 Create 命令后，选取随机秘密数 $r_{\mathrm{Y}}\in[2,n-1]$，计算 $D_{\mathrm{Y}}=(r_{\mathrm{Y}}+KS_{\mathrm{Y}})KP_{\mathrm{A}}$；并使用洋葱私钥对 $E\{KP_{\mathrm{Y}},D_2\}$进行解密得到 D_2，Y 计算与 Alice 间的会话密钥 $K_{(\mathrm{A,Y})}=KS_{\mathrm{Y}}^{-1}(r_{\mathrm{Y}}+\ KS_{\mathrm{Y}})D_2$；然后发送 Created 命令给 X，负载包括密钥协商信息 D_{Y} 和会话密钥 $K_{(\mathrm{A,Y})}$ 的散列值 $H(K_{(\mathrm{A,Y})})$；X 接收到 Created 命令后，创建 Extended 命令传输给 Alice，负载包括 D_{Y} 和 $H(K_{(\mathrm{A,Y})})$；Alice 收到 Extended 后，计算与 Y 间的会话密钥 $K_{(\mathrm{A,Y})}=KS_{\mathrm{A}}^{-1}(r_2+KS_{\mathrm{A}})D_{\mathrm{Y}}$，此时匿名链路扩展至中继节点 Y，同时完成会话密钥的协商，并且 Alice 基于会话密钥的散列值完成对密钥协商过程的完整性验证。

Alice 计算的会话密钥为

$$K_{(\mathrm{A,Y})}=KS_{\mathrm{A}}^{-1}(r_2+KS_{\mathrm{A}})D_{\mathrm{Y}}=(r_2+KS_{\mathrm{A}})(r_{\mathrm{Y}}+KS_{\mathrm{Y}})P$$

节点 Y 计算的会话密钥为

$$K_{(\mathrm{A,Y})}=KS_{\mathrm{Y}}^{-1}(r_{\mathrm{Y}}+KS_{\mathrm{Y}})D_2=(r_2+KS_{\mathrm{A}})(r_{\mathrm{Y}}+KS_{\mathrm{Y}})P$$

Alice 使用相同的策略将匿名链路拓展至其他中继节点，且相继与中继节点协商会话密钥，建立到达目标 Bob 的匿名通信链路。

3.4　匿名通信过程

匿名链路建立完成后，Alice 启动如算法 3 所示的匿名消息封装算法进行匿名通信数据的封装，匿名链路中各中继节点基于算法 4 所示的消息转发策略对其所接收的消息进行转发。通信数据在传输前首先被 Alice 的代理程序按匿名链路的中继节点顺序从后至前进行层层嵌套加密，加密后的匿名消息每通过一个中继节点被解密一次，直到目标 Bob 时匿名消息被完全解密；而响应数据从目的端返回的过程中，每经过一个中继节点被加密一次，最终经代理程序层层解密后转发给 Alice。

算法 3　匿名消息封装策略

Begin

① ***Data*** $=\boldsymbol{E}\{K_{(\mathrm{Alice,Bob})}$，***message***$\}$；

② ***Data***$=\boldsymbol{E}\{K_{(\mathrm{Alice,Node}_{(n)})}$，Bob 的伪装地址区间 $\|$ ***Data***$\}$；

③ **For** i=n-1 **to** i=1 //根据节点顺序封装匿名通信数据，倒序封装

Data$=\boldsymbol{E}\{K_{(\mathrm{Alice,Node}_{(i)})}$，节点 $\mathrm{Node}_{(i+1)}$的 IP 地址$\|$ ***Data***$\}$；

End For

④ $\mathbf{IP}_{\mathrm{Source}}=$ ***IP_XOR***$(\mathbf{IP}_{\mathrm{Alice}},\mathbf{IP}_{\mathrm{Bob}})$；//将编码地址作为匿名消息的源地址

⑤ 根据[目标地址，通信数据，源地址]的格式封装匿名通信数据；

End

算法 4　匿名消息转发策略

Begin

① 节点 Node_1 收到匿名通信数据 ***Data***；

② ***Data′*** $=\boldsymbol{D}\{K_{(\mathrm{Alice,Node}_{(1)})}$，***Data***$\}$；

③ 节点 $\mathrm{Node}_{(1)}$从 ***Data*** 中获得后继节点 $\mathrm{Node}_{(2)}$ 的 IP 地址，并将解封装后的 ***Data′*** 转发给 $\mathrm{Node}_{(2)}$；

④ **For** i=2 **to** i=n−1

节点 $\mathrm{Node}_{(j)}$获得节点 $\mathrm{Node}_{(j-1)}$发送的匿名通信消息；

Data′ $=\boldsymbol{D}\{K_{(\mathrm{Alice,Node}_{(i)})}$，***Data′***$\}$；

节点 $\mathrm{Node}_{(j)}$从 ***Data′*** 中获得节点 $\mathrm{Node}_{(j+1)}$ 的 IP 地址，并将解封装后的 Data′ 转发给 $\mathrm{Node}_{(j+1)}$；

End For

⑤ 节点 $\mathrm{Node}_{(n)}$获得 $\mathrm{Node}_{(n-1)}$发送的匿名通信消息；

⑥ **Data′** $=\boldsymbol{D}\{K_{(\mathrm{Alice,Node}_{(n)})}$，**Data′**$\}$；

⑦ 节点 $\mathrm{Node}_{(n)}$从消息 Data’中获得 Bob 的伪装地址区间，并发送解封装后的匿名通信消息给地址区间中的所有成员；

End

Bob 接收到匿名通信消息后，使用自己的 IP 地址可计算出发送方 Alice 的 IP 地址，即 $\mathbf{IP}_{\mathrm{Alice}}=$ ***IP_XOR***$(\mathbf{IP}_{\mathrm{Source}},\mathbf{IP}_{\mathrm{Bob}})$；同时使用与 Alice 间的协商密钥可解密通信消息，获得原始的通信明文。

3.5　恶意匿名行为控制策略

用户行为的信任评估是用户大量行为的体现，本文基于滑动窗口机制[18]提出用户行为信任的评

估策略，利用滑动窗口大小来体现用户行为信任评估的时间和空间特性，它既可以保证用户行为信任评估的规模性也可以保证行为信任评估的可扩展性，根据窗口记录的时间来保证近期行为的重要性和远期行为的衰减性，同时根据窗口的移动与更新来防止用户的欺骗等，窗口的基本结构如图 2 所示，每个行为属性由行为名称、行为发生时间、静态特征值、动态特征值和评估值构成。

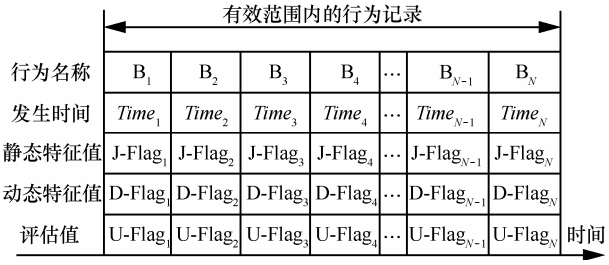

图 2 基于滑动窗口的行为标记记录机制

匿名链路的出口节点基于行为信任的监控机制获取匿名用户的行为特征值，通过行为特征值与 DC-ACS 设置的安全门限值间的比较触发相应的控制策略。

如图 3 所示的基于行为信任的监控机制中，静态可信度量模块主要检测用户行为操作的权限，并更新行为特征值记录的静态特征值属性；动态度量模块主要提交用户行为操作过程和结果的度量信任值，并更新动态特征值属性；安全性评估预测为控制仲裁对用户行为的可信性预测，同时更新评估值属性；即控制仲裁将动态模块和静态模块对用户行为的度量信任值量化为一个权值，量化的权值即为用户行为的特征值，并在量化过程中加入控制仲裁对用户行为的安全性评估值和用户的历史行为特征值。

当用户产生新的访问行为时，通过窗口的左移，把最左边的记录移出，新的信任值移入窗口的最右边，保证了行为评估模型的可扩展性及近期行为的主导性，同时根据式(1)更新用户的历史行为特征值 $Flag_{\mathrm{User}}$，且 $Flag_{\mathrm{User}}$ 的初始值为 0。

$$Flag_{\mathrm{User}}=\frac{Flag_{\mathrm{User}}+(\alpha T_{J[N]}+\beta T_{D[N]}+\gamma T_{U[N]})}{2} \tag{1}$$

其中，$T_{J[N]},T_{D[N]},T_{U[N]}\in[0,1]$。

如式(2)所示控制仲裁计算用户行为特征值时，每次行为的信任值在总特征值中所占的比例与该信任记录的时间成正比。

$$Trust_{\mathrm{Alice}}=(Flag_{\mathrm{User}}+\sum_{j=1}^{N}\frac{Time_j}{Time_j-Time_1}\cdot \sum_{i=1}^{N}\alpha T_{J[i]}+\beta T_{D[i]}+\gamma T_{U[i]})/(N+1) \tag{2}$$

其中，$T_{J[i]},T_{D[i]},T_{U[i]}\in[0,1]$。

$Trust_{\mathrm{Alice}}$ 表示是 Alice 的行为特征值；$T_{J[i]}$ 表示静态度量模块对用户行为的度量信任值；$T_{D[i]}$ 表示动态度量模块对用户行为的度量信任值；$T_{U[i]}$ 表示控制仲裁对用户行为的安全性评估值；N 为滑动窗口的大小；α、β、γ 分别表示百分比，且 $\alpha+\beta+\gamma=1$，针对不同行为的监控侧重点不同，调节 α、β 和 γ 的大小。若 Alice 是恶意匿名用户，则 Alice 的行为特征值 $Trust_{\mathrm{Alice}}$ 小于系统安全门限值 S，其中 $Trust_{\mathrm{Alice}}$、$S\in[0,1]$。

当用户长期无访问行为发生时，部分行为的信任记录距离当前时间越来越远，逐渐成为过期信任

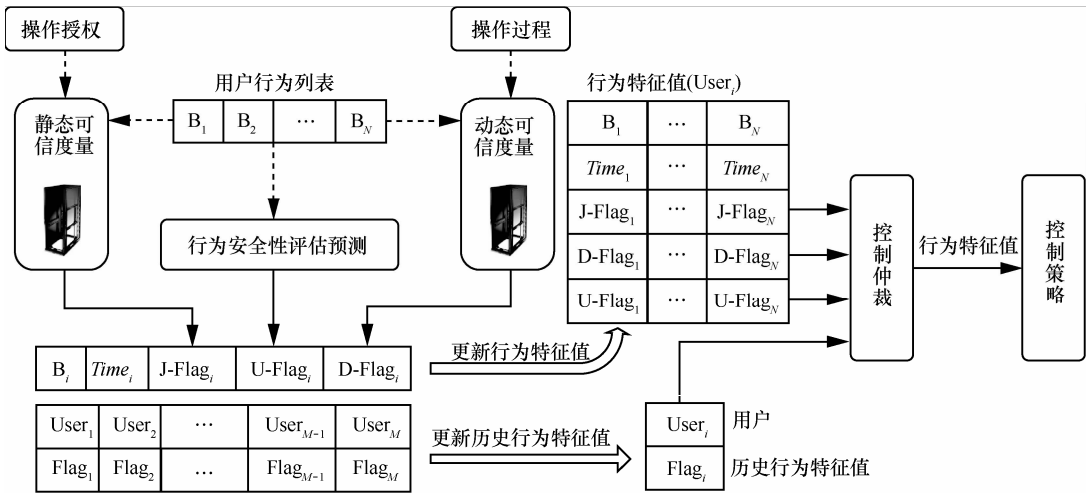

图 3 基于行为信任的监控机制

记录，信任是否过期是通过比较当前时间与各个记录时间的差是否大于有效时间段 Long_Time 来决定的，过期记录将被替换为初始信任值 Value_Init，这样随时间的推移信任会逐渐趋于 Value_Init。

由于行为的可信性监测已是安全控制领域的研究热点，众多研究者已在可信性监测方面进行了相关研究，并取得了大量研究成果[16,18,19]。

4　模型分析

4.1　匿名性分析

Alice 按其所通过转发节点的顺序从后至前用各中继节点的洋葱公钥对匿名数据进行层层嵌套加密，在传输过程中，加密后的数据每通过一个转发节点被解密一次，直到 Bob 数据被完全解密，增强了 Alice 和 Bob 及中继节点的身份、位置和通信的匿名性。

匿名链路中任意节点仅掌握直接前驱节点和后继节点的相关公开信息，并不能获知其他中继节点的身份信息，更无法获知 Alice 和 Bob 的身份信息，因此保证了 Alice 和 Bob 的身份匿名性。

通信数据按照路径中节点的顺序，从后至前依次用节点的洋葱公钥进行层层加密，每个转发节点仅能用自身的洋葱私钥解密数据后获知后继节点的地址信息，无法获知其他节点的地址，更不能获知 Alice 和 Bob 的地址信息，即中继节点无法准确判断 Alice 与 Bob 间的跳数；由于在匿名通信数据封装时对源地址进行了编码处理，对于匿名链路的入口节点而言，其所获悉的地址为编码处理后的地址信息，并非 Alice 的真实地址，对于匿名链路的出口节点而言，很难从众多接收者中准确猜测出 Bob 的具体地址，同时无法通过破解编码地址而得到 Alice 的地址，即匿名链路的入口节点和出口节点同样无法获悉 Alice 和 Bob 的具体地址信息。因此保证了 Alice 和 Bob 的位置匿名性。

匿名链路建立阶段，中继节点 X 发往后继节点 Y 的链路建立信息是经过节点 Y 的公钥加密的，只有节点 Y 才能解密获得相关信息，从而保证了通信的匿名性，也不能通过追踪信息包来发现 Alice 和 Bob，即第三方难以推断 Alice 与 Bob 间的通信模式，因此保证了 Alice 和 Bob 的通信匿名性。

综上所述，DC-ACS 中匿名链路的入口节点和出口节点无法获悉发送者和接收者的相关信息，发送者和接收者具有较强的匿名性，满足用户对匿名通信系统的基本要求—发送者匿名、接收者匿名和通信匿名。

4.2　安全性分析

4.2.1　抗中间人攻击

假设 Smart 是主动的攻击者且知晓 Alice 与中继节点 Node 间会话密钥协商过程的所有参数及相关算法。

① Smart 截获 Alice 发送的 $D_{\mathrm{A}}=(r_{\mathrm{A}}+KS_{\mathrm{A}})KP_{\mathrm{N}}$ 后，产生随机秘密数 $r_{\mathrm{S}}^{1}\in[2,n-1]$ 并计算密钥协商参数 $D_{\mathrm{S}}^{1}=(r_{\mathrm{S}}^{1}+KS_{\mathrm{S}})KP_{\mathrm{N}}$，将 D_{A} 替换为 D_{S}^{1}，并伪装成 Alice 将 D_{S}^{1} 发送给节点 Node；

② 节点 Node 接收到 D_{S}^{1} 后，随机选取秘密数 $r_{\mathrm{N}}\in[2,n-1]$，计算 $D_{\mathrm{N}}=(r_{\mathrm{N}}+KS_{\mathrm{N}})KP_{\mathrm{A}}$，并返回密钥协商参数 D_{N} 给 Alice；

③ Smart 截获 Node 的响应消息后，随机选取秘密数 $r_{\mathrm{S}}^{2}\in[2,n-1]$，并计算 $D_{\mathrm{S}}^{2}=(r_{\mathrm{S}}^{2}+KS_{\mathrm{S}})KP_{\mathrm{A}}$，将 D_{N} 替换为 D_{S}^{2}，并伪装成 Node 将 D_{S}^{2} 发送给 Alice。

Alice 计算的会话密钥(Alice 认为是与 Node 间的会话密钥)为

$$K_{(\mathrm{A,N})\mathrm{Alice}}=KS_{\mathrm{A}}^{-1}(r_{\mathrm{A}}+KS_{\mathrm{A}})D_{\mathrm{S}}^{2}=(r_{\mathrm{A}}+KS_{\mathrm{A}})(r_{\mathrm{S}}^{2}+KS_{\mathrm{S}})P$$

Node 计算的会话密钥(Node 认为是与 Alice 间的会话密钥)为

$$K_{(\mathrm{A,N})\mathrm{Node}}=KS_{\mathrm{N}}^{-1}(r_{\mathrm{N}}+KS_{\mathrm{N}})D_{\mathrm{S}}^{1}=(r_{\mathrm{N}}+KS_{\mathrm{N}})(r_{\mathrm{S}}^{1}+KS_{\mathrm{S}})P$$

攻击者 Smart 分别计算它与 Alice 和 Node 间的协商会话密钥 $K_{(\mathrm{S,N})}=KS_{\mathrm{S}}^{-1}(r_{\mathrm{S}}^{1}+KS_{\mathrm{S}})D_{\mathrm{N}}$ 和 $K_{(\mathrm{S,A})}=KS_{\mathrm{S}}^{-1}(r_{\mathrm{S}}^{2}+KS_{\mathrm{S}})D_{\mathrm{A}}$。

因为 $K_{(\mathrm{A,N})\mathrm{Alice}}\neq K_{(\mathrm{S,A})}$ 和 $K_{(\mathrm{A,N})\mathrm{Node}}\neq K_{(\mathrm{S,N})}$，所以攻击者 Smart 无法对密钥协商过程进行中间人攻击。

4.2.2　会话密钥的安全性

由于 Alice 与中继节点 Node 进行密钥协商时均使用不同的随机数，随机数的新鲜性保证了某一次会话密钥的泄露不会影响其先前或将来会话密钥的安全性。则会话密钥具有完美的前后向安全性。

Alice 与 Node 间的会话密钥是由随机数 r_{A} 和 r_{N} 共同产生，r_{A} 和 r_{N} 的随机性可确保密钥的新鲜性，并且任何一方面都无法单独计算出双方间的会话密钥。因此会话密钥具有新鲜性。

因为会话密钥计算过程中包含 Alice 和 Node 的私钥，由私钥的保密性保证了会话密钥的保密性。

4.2.3 抗攻击性分析

针对文献[20]定义的常见网络攻击方式，本文对 DC-ACS 的抗攻击性进行研究，如表 3 所示。

表 3 DC-ACS 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，但在终端处未保护
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进行评估
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

4.2.4 行为的信任评估机制

开始时用户行为信任记录窗口中每个信任值被初始化为 Value_Init；随着用户访问行为的发生，初始化值被移出窗口，逐渐记录用户访问行为的信任值。因此，本文机制可杜绝用户直接获取信任后而进行恶意访问行为。

窗口的大小是 N，当用户访问的次数 m 很大时，也仅记录最近 N 次访问行为的信任值，因此保证了信任评估的可扩展性。当欺骗者企图通过次数较少的高信任交互以获得较高的行为特征值时，由于总特征值是按窗口大小计算的，所以即使每次行为获得很高的信任评估值，由于实际交往的次数远比 N 小，所以并不能很快获得高信任值。因此，有效防止用户通过少数信任赢取最大的操作权限。

4.3 匿名度仿真

Reiter 和 Rubin 提出针对共谋攻击的匿名度分析方法[21]，攻击者由多个恶意节点组成，且每个恶意节点占据了不同的位置。本文研究的匿名链路均由非恶意者发起，同时接收者也为非恶意者。

假设匿名通信链路的长度均为 n，其中有 c 个恶意节点，则该链路中转发节点为有效节点的概率为 $P=1-\frac{c}{n}$；接收者伪装组中有 L 个成员，即接收者列表的容量为 L。

文献[22]详细介绍了匿名通信链路匿名度计算方法，根据文献[22]中所叙述的匿名度计算方法可得匿名通信链路的匿名度为 $d=\frac{(1-P)^2}{(1-P^{nP})(1-P^{nP-1})}$。

在 DC-ACS 中，匿名链路出口节点从接收者列表中准确猜测出接收者的概率为 $\frac{1}{L}$，然而对于入口节点而言，只有获得接收者的地址后，才能通过解码准确定位匿名消息的发送者，因此匿名链路的入口节点准确定位发送者的概率为 $\frac{1}{L}$，因此，DC-ACS 的匿名度为 $D=\frac{(1-P)^2}{L^2(1-P^{nP})(1-P^{nP-1})}$。

如图 4 所示，DC-ACS 的匿名度随匿名链路长度 n 的增大而减小，DC-ACS 的匿名性增强，但匿名链路长度 n 对匿名度的影响较小，因此为降低通信时延需选择较小的 n 值；DC-ACS 的匿名度随接收伪装组成员数 L 的增大而减小，且接收伪装组成员数 L 对匿名度的影响较大，因此为增强匿名性可选择较大的 L 值；如图 5 所示，DC-ACS 的匿名度随有效节点概率 P 的增大而减小，受 P 的影响较大。

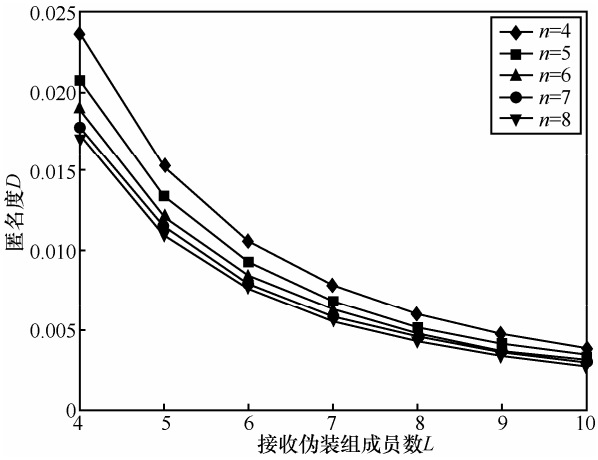

图 4 匿名链路的长度 n 对匿名度的影响（有效节点概率 P=0.5）

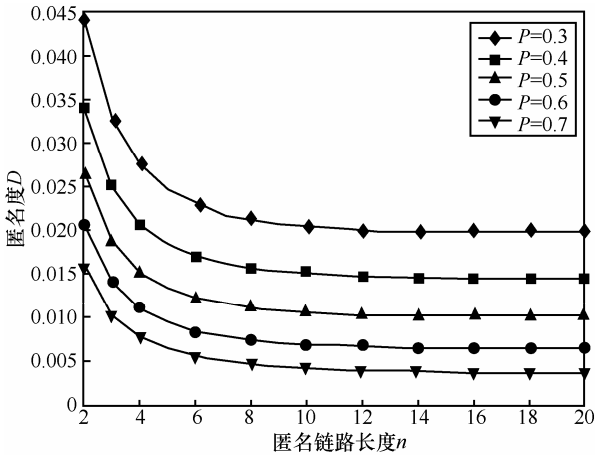

图 5 有效节点概率 P 对匿名度的影响（有效伪装组成员数 L=5）

由图 6 可知，当 $n\geqslant5$，$P\geqslant0.5$，$L\geqslant6$ 时匿名度大小趋近于 0，接近绝对匿名的等级，且此时匿名度大小不受匿名链路长度 n 的影响，受接收伪装组成员数 L 和有效节点概率 P 的影响较大。由于匿名链路的出口节点以广播的方式将匿名消息发送给接收伪装组中的每个成员，因此 L 的大小并不会增加通信时延，因此可选取较大的 L 以使 DC-ACS 取得更佳的匿名效果。综上所述，只需选择 n=5，$L\geqslant6$，只要有 50%以上的节点是可信节点 DC-ACS 即可满足发送者的强匿名性需求。

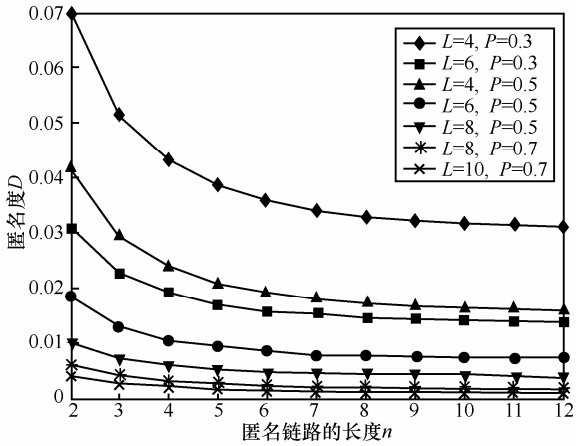

图 6　匿名度仿真

4.4　恶意匿名行为的可控性

在 DC-ACS 中，匿名链路的出口节点基于行为信任的监控机制对匿名用户的访问行为进行检测，当发现用户有恶意的匿名行为发生时，将触发相应的控制策略对匿名访问行为进行控制，减少用户恶意匿名行为对系统造成的危害。同时根据用户操作行为侧重点的不同，可动态调节行为信任值中各因素所占的比重，因此本文基于行为信任的监控机制具有动态调节的功能，且具有下述特点。

1) 近期行为的主导作用

行为特征值计算时单个行为信任值所占的比重根据时间的远近逐渐递增；同时，当有新的访问行为产生时，将最早进入滑动窗口的行为信任值移出，体现了近期行为对特征值的主导作用。

用户长时间没有访问行为发生时，滑动窗口中较早的行为信任值将因过期被移出，并由初始信任值替代，这样当用户长期没有访问行为时，行为特征值将随时间的推移逐渐趋于初始信任值，也体现了近期行为的主导作用。

2) 行为特征值的稳定性

若用户只有少数几次的访问行为，即使信任值均很高，其他的行为信任值即为初始信任值，由于行为特征值是通过全部 N 个信任记录计算的，所以行为特征值不会上升很快。体现了行为特征值的稳定变化的特性。

3) 行为特征值的灵活性

行为特征值计算过程中，由于每个行为信任值有静态度量值、动态度量值和安全性评估值 3 个方面组成，并且所占的比重大小不一，因此在计算时可根据访问行为的特点变化静态度量值、动态度量值和安全性评估值所占的比重，即行为特征值具有可调控的灵活性。

下面对 DC-ACS 中某次访问行为的特征值 $Flag=\alpha T_{J[N]}+\beta T_{D[N]}+\gamma T_{U[N]}$ 的度量过程进行仿真，并对仿真结果进行分析。

图 7 所示为行为特征值在不同 α、β、γ 的比例分配下的变化曲线。假设在正常情况下，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 7 中的图像区域即为行为特征值在不同分配比例下的变化曲线。当 α=1 时，行为特征值取得最大值 0.8；当 γ=1 时，行为特征值取得最小值 0.6，所以目标主机可以根据侧重点的不同动态的调节 α、β、γ 的比例，根据行为特征值的变化情况来选取合适的控制门限值 S。

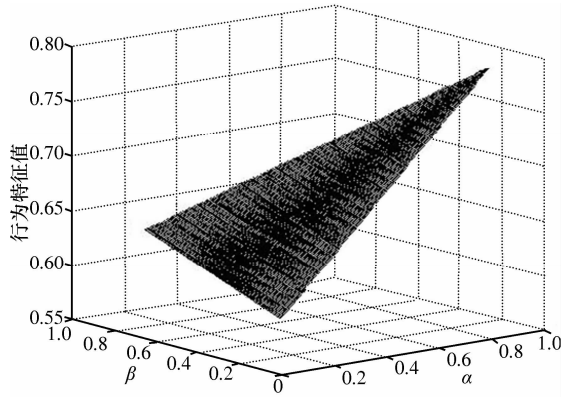

图 7　行为特征值在不同比例下的变化

图 8 所示为行为特征值在反馈触发过程中的变化曲线，其中，α=0.45，β=0.15，γ=0.4，行为的安全性评估信任值为 0.3，图 8 中的黑色区域即为该状态下的取值变化范围。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，行为特征值可以达到的最大值为 0.62。

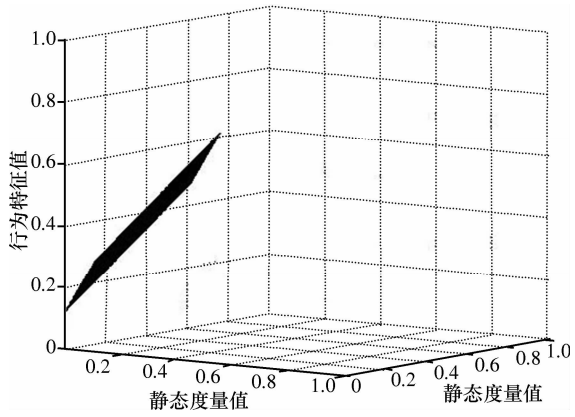

图 8 行为特征值在交互过程中的变化

4.5 技术对比

1) 性能比较

DC-ACS 与 Tor 匿名通信系统都采用嵌套加密的匿名通信模式，同时均基于一定数量的中继节点完成匿名链路的建立，因此 DC-ACS 的通信性能并不优于 Tor 匿名通信系统，与 Tor 的性能级别相同。

2) 安全性比较

本文将 DC-ACS 和 Tor 匿名通信系统在抗攻击性、可控性及会话密钥协商的安全性等方面进行了详细比较，比较结果如表 4 所示。分析表明 DC-ACS 较 Tor 而言，在具有恶意匿名行为可控性的同时，具有更高的安全性、匿名性及抗攻击能力。

表 4 DC-ACS 与 Tor 匿名通信系统技术比较

性能	DC-ACS	Tor 匿名通信系统
抗攻击性	抗攻击能力强	抗攻击能力适中
发送者匿名性	任何节点都无法获知发送者的身份信息，高匿名性	入口节点可掌握发送者的相关信息
接收者匿名性	任何节点都无法获知接收者的身份信息，高匿名性	出口节点可掌握接收者的相关信息
链路模式	链路具有多样性	链路的模式单一
可控性	具有匿名行为的可控性	不具备可控性
会话密钥的安全性	密钥协商过程可抵抗中间人攻击	密钥协商过程易受中间人攻击

5 结束语

本文 DC-ACS 中多样化匿名链路建立机制根据用户需求建立侧重不同的匿名通信链路，基于行为信任的控制机制完成对用户恶意匿名行为的控制，可防止用户的恶意匿名行为对 DC-ACS 造成危害，并且保证了发送者和接收者对匿名链路入口节点和出口节点的匿名性。通过与 Tor 匿名通信系统的比较，DC-ACS 在具有强匿名性的同时，具有更高的安全性和抗攻击的能力，解决了 Tor 匿名通信系统所存在的安全隐患。本文的主要创新工作有：① 多样化的匿名链路建立机制，用户可根据应用数据对传输链路匿名度和效率要求的不同，建立不同的匿名通信链路，增强了用户在匿名链路建立阶段的自主性；② 匿名链路的全匿名性，匿名链路的入口节点和出口节点都无法获知发送者和接收者的地址等相关隐私信息，增强了发送者和接收者的匿名性；③ 恶意匿名行为的可控性，匿名链路出口节点基于行为信任的监控控制机制，针对用户的恶意匿名行为制定相应的控制策略，防止用户恶意匿名行为的发生。

参考文献：

[1] CLAESSENS J, DIAZ C, GOEMANS C. Revocable anonymous access to the internet[A]. Internet Research: Electronic Networking Application and Policy[C]. 2003. 13-25.

[2] 吴艳辉,王伟平，陈建二. 匿名通信研究综述[J]. 小型微型计算机系统, 2007, 4 (5) : 583- 587.
WU Y H, WANG W P, CHEN J E. Anonymous communication: a survey[J]. Journal of Chinese Computer Systems, 2007, 4 (5): 583- 587.

[3] SERJANTOW A．Anonym zing censorship resistant systems[A]. Proc of the lst Int Peer-to-Peer Systems Workshop[C]. London, 2002. 111-120.

[4] GOLDSCHLAG D, REED M, SYVERSON P. Onion routing for anonymous and private Internet connections[J]. Communications of the ACM, 1999, 42(2): 39-41.

[5] DINGLEDINE R, MATHEWSON N, SYVERSON P. Tor: the second –generation onion router[A]. Proc of the 13th USENIX Security Symp[C]. Berkeley: USENIX Association, 2004.303-320.

[6] 陈周国, 蒲石, 祝世雄. 匿名网络追踪溯源综述[J]. 计算机研究与发展, 2012, 49(S2):111-117.
CHEN Z G, PU S, ZHU S X. Traceback technology for anonymous network[J]. Journal of Computer Research and Development, 2012, 49(S2): 111-117.

[7] REITER M K, RUBIN A D. Crowds: anonymity for Web transactions[J]. ACM Trans on Information and System Security, 1998, 1(1):66-92.

[8] FREEDMAN M J, MORRIS R. Tarzan: a peer-to-peer anonym zing net-work layer[A]. Proc of the 9th ACM Conf on Computer and Communications Security[C]. New York, USA, 2002. 193-206.

[9] DANEZIS G，DINGLEDINE R，MATHEWSON N. Mixminion: design of a type III anonymous remailer protocol[A]. Proc of the 2003 IEEE Symp on Security and Privacy[C]. Washington, IEEE Computer Society, 2003. 2-15.

[10] SHERWOOD R, BHATTACHARJEE B, SRINIVASAN A. P5: a protocol for scalable anonymous communication[J]. Journal of Computer Secu-rity, 2005, 13(6): 839-876.

[11] CHAUM D. The dining cryptographer’s problem: unconditional sender and recipient untraceability[J]. Journal of Cryptology, 1988, 1(1): 65-75.

[12] 陆天波. P2P 匿名通信协议 WonGoo 研究[D]. 北京: 中国科学院大学, 2006.
LU T B. Research on WonGoo—A Peer-to-Peer Anonymous Communication Protocol[D]. Beijing: Chinese University Academy of Sciences, 2006.

[13] 刘鑫. 基于 Tor 网络的匿名通信研究[D]. 上海: 华东师范大学，2011.
LIU X. Research on Anonymous Communication Based on Tor Network[D]. Shanghai: East China Normal University，2011.

[14] 杨元原. 一种混合的 Tor 通信系统方案[D]. 西安: 西安电子科技大学, 2007.
YANG Y Y. A Mixed Tor Anonymous Communication System Scheme[D]. Xi'an: Xi'an University of Electronic Science and Technology, 2007.

[15] 吴振强, 周彦伟, 乔子芮. 一种可控可信的匿名通信方案[J]. 计算机学报, 2010, 33(9): 1686-1702.
WU Z Q, ZHOU Y W, QIAO Z R. A controllable and trusted anonymous communication scheme[J]. Chinese Journal of Computers, 2010, 33(9): 1686-1702.

[16] 周彦伟, 吴振强, 蒋李. 分布式网络环境下的跨域匿名认证机制[J]. 计算机应用, 2010, 30(8): 2120-2124.
ZHOU Y W, WU Z Q, JIANG L. Cross-domain mecha-nismof anonymous attestation for distributed network[J]. Journal of Computer Applications, 2010, 30(8): 2120-2124.

[17] 周彦伟, 吴振强, 乔子芮. 可信匿名接入认证协议的研究与设计[J]. 计算机工程, 2011,37(5): 143-145.
ZHOU Y W, WU Z Q, QIAO Z R. Research and design of trusted anonymous authentication protocol[J]. Computer Engineering, 2011,37(5):143-145.

[18] 林闯, 田立勤, 王元卓. 可信网络中用户行为可信的研究[J]. 计算机研究与发展. 2008, 45(12):2033 -2043.
LIN C, TIAN L Q, WANG Y Z. Research on user behavior trust in trustworthy network[J]. Journal of Computer Research and Development, 2008, 45(12):2033-2043.

[19] 刘巍伟, 韩臻, 沈昌祥. 基于终端行为的可信网络连接控制方案[J]. 通信学报,2009,30(11):127-134.
LIU W W, HAN Z, SHEN C X. Trusted network connect control based on terminal behavior[J]. Journal on Communications, 2009, 30(11): 127-134.

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

[21] REITER M K, RUBIN A D. Crowds: anonymity for Web transactions[J]. ACM Transactions on Information and System Security, 1998, 1(1):62-92.

[22] 吴振强, 周彦伟, 马建峰. 物联网安全传输模型[J]. 计算机学报, 2011, 34(8): 1351-1364.
WU Z Q, ZHOU Y W, MA J F. A security transmission model for Internet of things[J]. Chinese Journal of Computers, 2011, 34(8): 1351-1364.

作者简介：

周彦伟（1986-），男，甘肃通渭人，陕西师范大学博士生，主要研究方向为密码学和匿名通信技术。

吴振强（1968-），男，陕西柞水人，博士，陕西师范大学教授、博士生导师，主要研究方向为匿名通信技术、网络安全、网络编码及应用。

杨波（1963-），男，陕西富平人，博士，陕西师范大学教授、博士生导师，主要研究方向为密码学和信息安全。