doi:10.11959/j.issn.1000-436x.2016178

基于 SDN 的电邮抵赖源头抑制方法

韩志耕[1,2]，冯霞[3]，陈耿[1,2]
（1. 南京审计大学工学院，江苏 南京 211815；2. 南京审计大学江苏省公共工程审计重点实验室，江苏 南京 211815；
3. 安徽大学计算机科学与技术学院，安徽 合肥 230601）

摘 要：受制于现有互联网体系可管控性的丧失，以签收电邮为代表的安全电邮技术仅能对电邮抵赖进行事后检测而无法实施源头抑制。基于 SDN（software-defined networking）控制与数据相分离的思想，通过将定制的抵赖抑制单元旁路附加到传统电邮模型之上，提出一种不破坏现有电邮结构的电邮抵赖源头抑制方法。在给出抵赖抑制单元内嵌的电邮证据绑定协议、抵赖行为检测算法、签收信度评估模型和抑制策略形成算法后，对所提方法在 4 种交叉场景中进行了有效性测试。实验结果表明，在与当前电邮系统兼容共生的前提下，所提方法能够对电邮抵赖实施有效的源头抑制。

关键词：电邮抵赖；源头抑制；SDN；签收电邮
中图分类号：TP393 **文献标识码**：A

SDN based e-mail repudiation source restraining method

HAN Zhi-geng[1,2], FENG Xia[3], CHEN Geng[1,2]
(1. Institute of Technology, Nanjing Audit University, Nanjing 211815, China;
2. Jiangsu Key Laboratory of Public Project Audit, Nanjing Audit University, Nanjing 211815, China;
3. School of Computer Science and Technology, Anhui University, Hefei 230601, China)

Abstract: With the limitation of controllability of the existing Internet architecture, the existing secure e-mail technology such as certified e-mail can only post detection but cannot source restraining on e-mail repudiation. Based on the idea of control and data separation of software-defined networking technology, by means of bypass attaching customized repudiation restrain unit to the traditional e-mail model. An e-mail repudiation source restraining method was proposed without destroying the existing e-mail structure. After presenting e-mail evidence binding protocol, repudiation behavior detection algorithm, certified reputation evaluation model, and repudiation restraining strategy formation algorithm embedded in repudiation restrain unit, the effectiveness were tested of the proposed method in 4 cross scenarios. The experimental results show that, under the premise of compatibility with the current e-mail system, the method can source restrain e-mail repudiation effectively.

Key words: e-mail repudiation, source restraining, SDN, certified e-mail

1 引言

虽然在过去 10 多年里电邮作为人与人之间沟通平台的基本属性不断地被削弱，但其所拥有的特有通信优势使其依然保持着较广的应用[1]。2014 年 Gartner安全电邮网关魔力象限显示，电邮话题讨论

收稿日期：2016-02-28；**修回日期**：2016-07-12
通信作者：冯霞，fengx.ahu@foxmail.com
基金项目：国家自然科学基金资助项目（No.71271117）；江苏省自然科学基金资助项目（No.BK20151460）；江苏省高校自然科学基金资助项目（No.16KJB520021）；江苏省网络与信息安全重点实验室基金资助项目（No.BM2003201）；江苏省公共工程审计重点实验室开放课题基金资助项目（No.GGSS2015-04）
Foundation Items: The National Natural Science Foundation of China (No.71271117), The Natural Science Foundation of Jiangsu Province (No.BK20151460), The University Natural Science Foundation of Jiangsu Province(No.16KJB520021), Jiangsu Province Key Laboratory of Network and Information Security(No.BM2003201), The Opening Foundation of Jiangsu Province Key Laboratory of Public Project Audit (No.GGSS2015-04)

的严肃性使目前 80%的工作交互主要借助其进行；电邮通信记录的法律效应使其在电子政务等诚信敏感领域具有当前新兴工具无法企及的重要地位。即便在移动互联网时代，电邮仍表现出极好的平台适应性，2013 年上线即获好评的Ping应用就是例证。尽管如此，电邮发展仍面临诸多困境，且安全问题是首要问题。2013 年Gartner报告将安全电邮列入最抢手云安全服务行列，并预测 2017 年其市场份额会迈进 10 亿美元大关。

作为一种典型的电邮安全威胁，电邮抵赖是对先前电邮交互事实的拒绝承认，包括电邮发送抵赖和接收抵赖。当前抑制电邮抵赖的主要技术是签收电邮[2]，其通过在不信任的电邮主体之间公平地交换电邮信息和抗抵赖证据以实现电邮交互行为的可追溯[3]。签收电邮抑制电邮抵赖的方法是事后检测，这意味着被检测出的电邮抵赖可能已经奏效，对诚实用户或许已经形成伤害，从维护诚实用户利益的角度出发，倘若能从源头上抑制电邮抵赖，会减轻此类伤害，然而这在现有互联网体系内无法获得解决，原因在于：事后检测电邮抵赖无须对电邮交互进行在线干预，但源头抑制必须强加在线控制，而现有互联网可管性的丧失却无法为之提供保障。当前互联网细腰模型正被打破，各种协议决策逻辑交织在一起产生的非线性作用使网络行为呈现出复杂性且难以预测[4]。本文充分发挥 SDN 在提升网络安全上的优势[5]，基于其控制与数据相分离的思想，通过将定制的电邮抵赖抑制单元旁路附加到传统电邮模型之上，提出一种不破坏现有电邮结构的电邮抵赖源头抑制方法。

2 相关工作

传统邮政系统中抑制邮件抵赖的主要手段是采用给据邮件。与给据邮件中抗抵赖证据（即手签纸质给据）容易获取不同，电邮系统中抗抵赖证据的获取却极其困难。事实上，受制于现有互联网体系对可审计性的不支持[6]，诸如S/MIME (secure/multipurpose Internet mail extensions)等电邮安全协议虽然能提供完整性、认证性和保密性，但均无法提供抗抵赖性；尽管RFC2634 通过将签收证据引入S/MIME以提供电邮抗抵赖问题，但其建立在收件人定会返回收条的假设之上，在真实世界中通常难以满足[2]。

受给据邮件思想启发，当前抑制电邮抵赖的主要技术是签收电邮，研究的焦点为如何在可审计性缺失的互联网体系内进行电邮取证，相关研究集中在以下 3 个方面，分别为电邮取证的公平性、环境适应性和互操作性。

1) 电邮取证公平性旨在保证所有电邮实体要么都能获得想要的证据，要么都无法获得对己有利的证据[3]，其理论基础是公平交换[7]。Onieva等[8]将异步时限性技术引入文献[9]中的快速乐观签收电邮协议，使所有实体可在协议执行的任意阶段终止执行而不破坏取证的公平性；Shao等[10]针对回放攻击可致诚实方无法获得期望的电邮证据的问题，提出规避回放攻击的指导原则；Payeras-Capella等[11]针对选择性接收会致发送方丢失证据的问题，通过推迟暴露发送方签名给出无选择性接收的公平签收电邮协议。

2) 在电邮取证环境适应性方面，Puigserver等[12]和Ateniese等[13]分别提出基于第三方联盟和第三方任务划分的信任弱化技术，解决了先前电邮取证对第三方信任的强依赖问题；Zhou等[14]通过扩展两方签收电邮协议提出具备一对多通信拓扑的多方变体协议，解决了电邮群发中多主体间的公平取证问题；王彩芬等[15]通过简化取证消息步与密码操作提出适用于资源受限网络（如无线移动网）的低开销签收电邮协议。

3) 互操作性是指异构签收电邮系统为达成跨系统公平取证而进行的差别互补与兼容共生，这是在异构环境下大规模部署签收电邮系统需要解决的问题[2]。Tauber等提出了签收电邮互操作标准[16]、建立了签收电邮跨欧盟互操作方案[17]，同时还设计出符合传统电邮体系的互操作乐观签收电邮协议[18]；Paulin等[19]提出一种概率公平签收电邮系统，解决了因可信第三方带来的签收电邮应用范围有限和无法跨国互操作的问题。

虽然签收电邮技术在可审计性缺失的互联网体系内借助电邮取证实现了对电邮抵赖的事后检测，然而受制于现有互联网体系可管控性的缺失[20]，该技术因为无法对电邮抵赖实施在线控制，从而无法对其实施源头抑制。与签收电邮技术相比，本文利用 SDN 控制与数据相剥离的思想，通过将定制的抵赖抑制单元旁路附加到现有电邮模型之上，实现了电邮数据逻辑与抵赖抑制逻辑的剥离，为电邮抵赖在线控制提供了途径，并进而解决了现有技术对电邮抵赖仅能事后检测而无法源头抑制的问题。

3　源头抑制框架

3.1　基本构想

本文源头抑制电邮抵赖的基本构想如下：电邮系统最初处于诚信稳定态（即无抵赖）；当电邮抵赖发生后系统由诚信稳定态迁移到抵赖扰动态；进而由于抵赖抑制策略的激活实施，系统由抵赖扰动态迁移到抵赖控制态；此后随着电邮抵赖的不断出现和抵赖抑制的自适应实施，系统经由若干抵赖抑制中间态（即扰动态与控制态的切换与调整），并最终回归到诚信稳定态。该构想的实现要求电邮系统必须具备可控性，以便将电邮抵赖抑制策略（即控制逻辑）在线作用于电邮交互（即数据交互），这需要得到SDN技术[21]的支持。

SDN 由 Mckeown 教授于 2009 年在 INFOCOM 会议上提出，该技术通过将特定的网络硬件与软件进行解耦，实现了网络控制平面和数据平面的分离[20]，为提升网络可管控性提供了创新性方案。其中，控制平面掌握全局网络信息，采用具有逻辑中心化和可编程的控制器，方便管理配置网络和部署新协议；数据平面仅提供简单的数据转发功能，采用哑交换机，用于快速处理匹配的数据分组；控制器通过 OpenFlow 等标准接口向交换机下发转发规则，交换机仅需按照这些规则执行相应的转发动作。

3.2　方法框架

基于 SDN 技术，一种可行的电邮抵赖源头抑制方法框架如图 1 所示，其特征在于通过给传统电邮模型旁路附加一个抵赖抑制单元包括行为证据绑定组件、行为证据管理组件、抵赖程度评估组件、签收信度管理组件和抑制策略生成组件，从而实现电邮抵赖行为的可抑制、可管理。在该方法的闭环自反馈框架内，从电邮交互前的抵赖避免，到电邮交互中的抵赖取证，再到电邮交互后的抵赖评估，整个过程使电邮交互成为一个自适应运行的抵赖抑制系统，满足了电邮交互的诚信需求。其中，传统电邮模型对应于 SDN 数据平面，用于标识基于传统电邮协议进行的电邮交互行为；抵赖抑制单元对应于 SDN 控制平面，用于对电邮抵赖行为实施抑制。

3.3　抑制流程

图 1 所述的电邮抵赖源头抑制方法的闭环抑制流程描述如下。

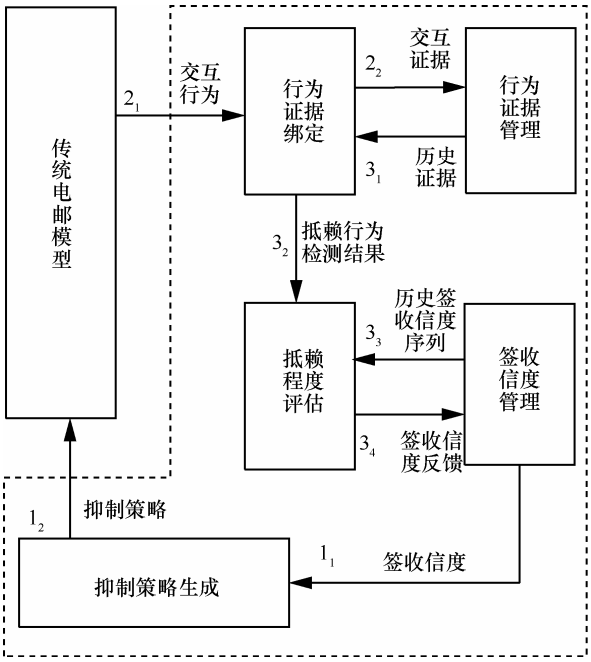


图 1　电邮抵赖源头抑制方法框架

1) 电邮交互之前的抵赖避免阶段。如图 1 的 1_1抑制策略生成组件依据签收信度管理组件提交的电邮实体最新签收信度形成抵赖抑制策略，并如图 1 的 1_2作用于传统电邮模型以调整即将进行的电邮交互。即

$$ISF(A,\{B_i\},\{cr_{A|\{B_i\}}\}^{t-1},t)=>\{ris_{A|\{B_i\}}\}^t \quad (1)$$

$$ISI(\{ris_{A|\{B_i\}}\}^t,\{b'_A\}^t|\{b'_{\{B_i\}}\}^t)=>\{b_A\}^t|\{b_{\{B_i\}}\}^t \quad (2)$$

其中，$ISF(\cdot)$为抑制策略形成算法，A 为电邮发送方，$\{B_i\}$为电邮接收方 $B_i(i\geqslant 0)$的集合，t 为协议轮标识，$\{cr_{A|\{B_i\}}\}^{t-1}$ 为 $t-1$ 轮电邮交互后电邮收发方的签收信度，=>为输出（下同），$\{ris_{A|\{B_i\}}\}^t$ 为针对 t 轮电邮交互的抵赖抑制策略。式(2)中，$ISI(\cdot)$为抑制策略实施函数，$\{b'_A\}^t|\{b'_{\{B_i\}}\}^t$ 为抵赖抑制策略未发生作用时欲进行的 t 轮电邮行为，$\{b_A\}^t|\{b_{\{B_i\}}\}^t$ 为抵赖抑制策略作用后所表现出来的 t 轮电邮行为。

2) 电邮交互之中的抵赖取证阶段。如图 1 的 2_1行为证据绑定组件对感知到的电邮交互行为实施不可否认证据绑定，如图 1 的 2_2，其结果以交互证据的形式提交给行为证据管理组件实施证据链管理。即

$$\mathrm{BbindE}(\{b_A\}^t|\{b_{\{B_i\}}\}^t)=>\{evdn_A\}^t|\{evdn_{\{B_i\}}\}^t \quad (3)$$

$$EchainM(\{evdn_A\}^t|\{evdn_{\{B_i\}}\}^t,\{<x\leftarrow y>_{A|\{B_i\}}\}^{t-1})=>\{<x\leftarrow y>_{A|\{B_i\}}\}^t \quad (4)$$

其中，式(3)中 $\mathrm{BbindE}(\cdot)$为证据绑定机制，$\{b_A\}^t|\{b_{\{B_i\}}\}^t$ 为感知到的 t 轮电邮行为，$\{evdn_A\}^t|\{evdn_{\{B_i\}}\}^t$为绑

定后的电邮证据；式(4)中 $EchainM(\cdot)$为证据管理算法，$\{<x\leftarrow y>_{A|\{B_i\}}\}^{t-1}$ 为 $t-1$ 轮交互后所形成的证据链，$\{<x\leftarrow y>_{A|\{B_i\}}\}^{t}$ 为 t 轮交互后形成的新证据链。

3) 电邮交互之后的抵赖评估阶段。如图 1 的 3_1行为证据绑定组件依据行为证据管理组件提供的历史交互证据对 t 轮交互行为实施抵赖检测，并如图 1 的 3_2将检测结果提交给抵赖程度评估组件。如图 1 的 3_3抵赖程度评估组件依据抵赖检测结果和签收信度管理组件提供的历史签收信度对 t 轮电邮实体抵赖程度进行评估，如图 1 的 3_4以签收信度形式反馈给签收信度管理组件，用于 $t+1$ 轮电邮交互前的抵赖避免。即

$$DER(\{<x\leftarrow y>_{A|\{B_i\}}\}^{t}) \Rightarrow \{res_{A|\{B_i\}}\}^{t} \tag{5}$$

$$CRC(\{res_{A|\{B_i\}}\}^{t}, <\{cr_{A|\{B_i\}}\}^{1}, \{cr_{A|\{B_i\}}\}^{2}, \cdots, \{cr_{A|\{B_i\}}\}^{t-1}>) \Rightarrow \{cr_{A|\{B_i\}}\}^{t} \tag{6}$$

其中，式(5)中 $DER(\cdot)$是抵赖检测算法，$\{res_{A|\{B_i\}}\}^{t}$ 为 t 轮电邮交互的抵赖检测结果；式(6)中 $CRC(\cdot)$是签收信度评估算法，$<\{cr_{A|\{B_i\}}\}^{1}, \{cr_{A|\{B_i\}}\}^{2}, \cdots, \{cr_{A|\{B_i\}}\}^{t-1}>$为第 1 轮到 $t-1$ 轮签收信度所构成的序列，$\{cr_{A|\{B_i\}}\}^{t}$ 为 t 轮签收信度。

4 抵赖抑制逻辑

4.1 电邮证据绑定

定义 1 电邮行为(EB, e-mail behavior) 限指电邮发送方与接收方之间为传递电邮内容所进行的通信交互，包括电邮发送行为与接收行为。

定义 2 电邮证据(EE, e-mail evidence) 指与电邮行为唯一关联的、可用于向非当事方重现电邮行为事实的抗抵赖电子凭证，包括电邮发送证据和接收证据。

本文定制的电邮证据绑定协议 BbindE 是对文献[14]的改进，其基本思想是在单向端到端的电邮内容传递的同时进行双向端到端的特征秘密交换。BbindE 包括 main 主协议和 abort 与 resolve 这 2 个辅助协议。

4.1.1 协议符号

A、B、TTP、M: 电邮发送方、既定接收方 B_i 集合、可信第三方、电邮内容。

B'：成功执行 main 协议步骤②的 B_i 集合，为 B 子集。

$B''=B-B'$：被 A 取消接收权的 B_i 集合，为 B 子集。

$B''\_cancelled$：被 TTP 取消接收权的 B_i 集合，为 B''子集。

$B''\_finished$：求助 resolve 协议恢复接收权的 B_i 集合，为 B 子集。

$S_X(M)$：实体 X 对 M 的数字签名。

$P_X(M), E_K(M)$：用实体 X 公钥对 M 进行非对称加密、用密钥 K 对 M 进行对称加密。

$P_B(M)= P_{B_1}(M), P_{B_2}(M), \cdots =E_K(M), P_{B_1}(K), P_{B_2}(K), \cdots$：集合 B 对 M 进行群加密。

$Z=P_{TTP}(A, B, P_B(M))$：特征秘密 Z。

$L=h(M)$：协议轮新鲜标签，h 为单向散列函数。

4.1.2 协议描述

1) 正常情形：电邮证据绑定仅使用 main 协议即可完成，无需 TTP 参与。

main 协议如下。

① $A \Rightarrow B$：$Z, L, S_A(Z, L)$

② $B_i \rightarrow A$：$L, S_{B_i}(Z, L)$

③ $A \Rightarrow B'$：$P_{B'}(M), L$

2) Z 交换异常：若 A 执行完 main 协议步骤①后未收到某些既定 $B_i \in (B''=B-B')$的反馈签名 $S_{B_i}(Z, L)$，A 执行 abort 协议以放弃与这些 B_i 的交互。

abort 协议如下。

① $A \rightarrow TTP$：$P_{TTP}(B''), Z, L, S_A(cancel, B'', Z, L)$

② TTP：for (all $B_i \in B''$) {

if ($B_i \in B''\_finished$) then retrieves $S_{B_i}(Z, L)$;

else appends B_i into $B''\_cancelled$ }

③ $TTP \rightarrow A$: all retrieved $S_{B_i}(Z, L)$, $B''\_cancelled$, $S_{TTP}(B''\_cancelled, Z, L)$, L

3) M 传递异常：若 B_i 执行完 main 协议步骤②后未收到 $P_{B_i}(M)$或 M 被篡改，B_i 可执行 resolve 协议以恢复交互。

resolve 协议如下。

① $B_i \rightarrow TTP$: $Z, L, S_{B_i}(Z, L)$;

if ($B_i \in B''\_cancelled$) then

② $TTP \rightarrow B_i$: $B''\_cancelled$, $S_{TTP}(B''\_cancelled, Z, L), L$;

else { $TTP \rightarrow B_i$: $P_{B_i}(M), L$;

TTP: appends B_i into $B''\_finished$, and stores $S_{B_i}(Z,L)$ }

BbindE 借助引入新鲜标签 $L=h(M)$并重构签名消息(如将 $S_{B_i}(Z)$重构为 $S_{B_i}(Z,L)$)，消除了原协议[14]因 A 恶意变更 M 给 B_i 带来的危害。原协议中 A 可在 main 协议步骤③中将步骤①中既定的 M 变更为 M'，最终 A 持有 B_i 接收 M 的证据，而 B_i 实际收到

的确为 M'，这对 B_i 来说不公平。BbindE 执行完后，A 持有电邮接收证据{$S_{B_i}(Z,L)$, $S_{TTP}(B''\_cancelled, Z, L)$}，$B_i$ 持有电邮发送证据{$S_A(Z,L)$,$S_{TTP}(B''\_cancelled, Z, L)$}

4.1.3 有效性证明

定理 1　BbindE 绑定证据可使仲裁方 J 相信电邮行为无否认。

证明　拟采用基于信仰的模态逻辑 SVO[22]进行证明如下。

BbindE 中基本项集为{{A, B_i, TTP, J}，{Z, L, M}，{K_A, K_{B_i}, K_{TTP}, K_A^{-1}, $K_{B_i}^{-1}$, K_{TTP}^{-1}, K}}

BbindE 中密钥持有假设 P_1 和 P_2 为

P_1 1) J believes $PK_\sigma(A, K_A)$　2) J believes $PK_\sigma(B_i, K_{B_i})$　3) J believes $PK_\sigma(TTP, K_{TTP})$

P_2 1) J believes (B_i *has* K_A)　2) J believes (B_i *has* K_{TTP})　3) J believes (A *has* K_{B_i})

BbindE 中证据提交假设 P_3 和 P_4 为

P_3 J believes J received {$S_{B_i}(Z, L)$, $S_{TTP}(B''\_cancelled, Z, L)$}

P_4 J believes J received {$S_A(Z, L)$, $S_{TTP}(B''\_cancelled, Z, L)$}

BbindE 中 TTP 称职假设 P_5 和 P_6 为

P_5 J believes (TTP said ($B''\_cancelled$, Z, L) ⊃ TTP received ($S_A(cancel, B'', Z, L)$))

P_6 J believes (TTP said ($B''\_cancelled$, Z, L) ⊃ TTP received $S_{B_i}(Z, L)$)

BbindE 中证据检索假设 P_7 和 P_8 为

P_7 J believes (TTP said ($B''\_cancelled$, Z, L) ⊃ A received $S_{TTP}(B''\_cancelled,Z,L)$)

P_8 J believes (TTP said ($B''\_cancelled$, Z, L) ⊃ B_i received $S_{TTP}(B''\_cancelled,Z,L)$)

BbindE 中理性接收人假设 P_9 和 P_{10} 为

P9 J believes (A said $PB_i(M)$ ⊃ A received $SB_i(Z, L)$)

P_{10} J believes (B_i said (Z, L) ⊃ B_i received $S_A(Z, L)$)

BbindE 中数据复原假设为 P_{11} 和 P_{12} 为

P_{11} J believes (A said $E_K(M) \wedge A$ said $K \supset A$ said M)

P_{12} J believes (B_i received $E_K(M) \wedge B_i$ received $K \supset B_i$ received M)

BbindE 协议目标 G_1 和 G_2 为

G_1 J believes (A said $M \wedge A$ received {$S_{B_i}(Z,L)$, $S_{TTP}(B''\_cancelled,Z,L)$})

G_2 J believes (B_i received $M \wedge B_i$ received {$S_A(Z,L)$, $S_{TTP}(B''\_cancelled, Z, L)$})

在假设 P_1~P_{12} 的基础上，结合 SVO 逻辑的 Nec 规则和信任公理、源关联公理、接收公理以及叙述公理可以证明 G_1 和 G_2 目标成立，逻辑推理过程略。　　证毕

4.2 抵赖行为检测

定义 3　电邮抵赖(ER, e-mail repudiation)指电邮实体出于私利对已实施的电邮行为予以否认，包括电邮发送抵赖(如 A 向 B_i 发送 M，但 A 事后否认曾发送过 M 给 B_i)和电邮接收抵赖(如 B_i 收到 A 发送的 M，但 B_i 事后否认曾接收过来自 A 的 M)。

以实体 A 向群体 B 发送电邮 M 为例，此处基于 4.1 节中证据绑定结果给出行为证据绑定组件内嵌的电邮抵赖检测算法，描述如下。

1) 发送方抵赖检测

发送方抵赖包括 2 种情况：A 未向 B_i 发送过 M 但宣称发送过，以及发送过但宣称未发送过。由于前者无法提供绑定证据，此处仅对后者展开检测，详见算法 1。

算法 1　*DER_sender*　// 发送方抵赖检测

输入　$CESB_A$ // 发送方宣称行为，0=未发送 M，1=发送了 M

$S_A(Z,L)$, $S_{TTP}(B''\_cancelled, Z, L)$ // 电邮发送证据

Z, L, B, $B''\_cancelled$, M, $P_{B_i}(M)$, $P_B(M)$ // 附加信息

输出　SR//发送方抵赖检测结果，0=抵赖，1=诚实

① $RESB_A$←0; SR←0; // 初始化真实行为变量和检测结果变量

② if $B_i \in B$ and $P_{B_i}(M) \in P_B(M)$ then {

③　if $Z==P_{TTP}(A, B, P_B(M))$ then {

④　if $L==h(M)$ then {

⑤　if $S_A(Z,L)$ is valid then {

⑥　if $S_{TTP}(B''\_cancelled, Z, L)$ is valid then {

⑦　if $B_i \notin B''\_cancelled$ then $RESB_A$←1; }}}}}

⑧ if $RESB_A==CESB_A$ then SR←1;

⑨ return SR;

2) 接收方抵赖检测

同理，此处仅对 B_i 接收来自过 M 但宣称未接收过进行抵赖检测，详见算法 2。

算法 2 *DER_receiver* // 接收方 *Bi* 抵赖检测

输入 $CERB_{B_i}$ // 接收方宣称行为，0=未收到 *M*，1=收到了 *M*

$S_{B_i}(Z,L)$, $S_{TTP}(B''\_cancelled, Z, L)$ // 电邮接收证据

Z, *L*, *B*, *B*″_*cancelled*, *M*, $P_{B_i}(M)$, $P_B(M)$ // 附加信息

输出 *RR* // 接收方抵赖检测结果，0=抵赖，1=诚实

① $RERB_{B_i}\leftarrow 0$; $RR\leftarrow 0$; // 初始化真实行为变量和检测结果变量

② if $B_i\in B$ and $P_{B_i}(M)\in P_B(M)$ then {

③ if $Z==P_{TTP}(A, B, P_B(M))$ then {

④ if $L==h(M)$ then {

⑤ if $S_{B_i}(Z,L)$ is valid then {

⑥ if $S_{TTP}(B''\_cancelled, Z, L)$ is valid then {

⑦ if $B_i\notin B''\_cancelled$ then $RERB_{B_i}\leftarrow 1$; }}}}}

⑧ if $RERB_{B_i}==CERB_{B_i}$ then $RR\leftarrow 1$;

⑨ return *RR*;

4.3 签收信度评估

4.3.1 评估步骤

定义 4 签收行为(CB, certified behavior) 特指电邮实体对电邮行为事实的诚实宣称或拒绝承认。

定义 5 签收信度(CR, certified reputation) 特指公众对电邮实体无抵赖签收行为的社会认可度。

签收信度的评估分 2 步完成，介绍如下。

1) 签收信度初估：基于抵赖检测结果计算初始签收信度，即 $RCR_t=f(SR_t, RR_t)$，其中，RCR_t为 *t* 轮初始签收信度，SR_t和 RR_t为 *t* 轮抵赖检测结果，$f(\cdot)$为签收信度初估模型。

2) 签收信度重估：对 RCR_t进行矫正以提升签收信度与真实签收行为的逼近度，即 $CR_t=g(RCR_t)$，其中，CR_t为 *t* 轮重估签收信度，$g(\cdot)$为签收信度重估模型。

由于可直接应用于签收信度初估的模型有很多[23]，故此处仅给出签收信度重估模型，描述如下

$$CR_t=\alpha RCR_t+\beta H_t+\gamma D_t+\delta D_t|SD_t|,\ 0<\alpha<1,\ 0<\beta<1,\ 0<\gamma<1,\ 0<\delta<1 \tag{7}$$

该模型改进文献[24]，但较原模型增添了时效维 $\delta D_t|SD_t|$，其利用 4 类数据(初始签收信度 RCR_t、历史签收信度 H_t、签收信度波动率 D_t和签收信度波动趋势 SD_t)对 RCR_t进行重估。式(7)中分量 H_t、D_t、SD_t计算方法如式(8)~式(10)所示。

$$H_t=\frac{1}{LH}\int_{t-LH}^{t-1}CR_x\mathrm{d}x\approx\frac{\sum_{k=t-LH}^{t-1}CR_k\rho^{t-(k+1)}}{\sum_{i=t-LH}^{t-1}\rho^{t-(i+1)}} \tag{8}$$

$$D_t=\sqrt{\frac{\sum_{k=t-LH}^{t-1}\left(CR_k-\sum_{i=t-LH}^{t-1}\frac{CR_i}{LH}\right)^2}{LH}}\approx RCR_t-H_t \tag{9}$$

$$SD_t=\sqrt{\frac{\sum_{k=t-LDH}^{t-1}\left(D_k-\sum_{i=t-LDH}^{t-1}\frac{D_i}{LDH}\right)^2}{LDH}}\approx D_t-\sum_{k=t-LDH}^{t-1}D_k\frac{\theta^{t-(k+1)}}{\sum_{i=t-LDH}^{t-1}\theta^{t-(i+1)}} \tag{10}$$

其中，式(8)中 $\rho(0<\rho\leqslant 1)$和 *LH* 分别为历史近邻签收信度的关注因子和关注时隙个数，式(10)中 $\theta(0<\theta\leqslant 1)$和 *LDH* 分别为历史近邻签收信度波动率的关注因子和关注时隙个数，且 *LH* 和 *LDH* 通常设置为电邮实体策略抵赖行为的振荡时隙大小；式(7)中α和β在设置上要求$\frac{\beta}{\alpha}$正比于 *LH*，且 γ 和 δ 在设置上拟遵循式(11)和式(12)。

$$\gamma=\begin{cases}\gamma_1, & D_t\geqslant 0\\ \gamma_2, & D_t<0\end{cases},\quad \gamma_1\leqslant\gamma_2 \tag{11}$$

$$\delta=\begin{cases}\delta_1, & D_t\cdot SD_t<0\\ \delta_2, & D_t\cdot SD_t\geqslant 0\end{cases},\quad \delta_1\leqslant\delta_2 \tag{12}$$

4.3.2 逼近度分析

定义 6 签收距离(CD, certified distance)。给定签收行为 $CB_t(0\leqslant CB_t\leqslant 1)$和对应的签收信度 $CR_t(0\leqslant CR_t\leqslant 1)$，则对应的签收距离为 $CD_t=|CR_t-CB_t|$。

定义 7 签收信度逼近度(DACR, degree of approximation of certified reputation)。给定签收行为 $CB_t(0\leqslant CB_t\leqslant 1)$和对应的签收距离 CD_t，则签收信度逼近度 $DACR_t=1-\frac{CD_t}{CB_t}$。

定理 2 在签收信度重估模型中引入时效维 $\delta D_t|SD_t|$可提高签收信度逼近度。

证明 设 $CB_t(0\leqslant CB_t\leqslant 1)$为签收行为，$CR'_t(0\leqslant CR'_t\leqslant 1)$为引入 $\delta D_t|SD_t|$之前获得的签收信

度，对应签收距离 $CD'_t=|CR'_t-CB_t|$，签收信度逼近度为 $DACR'_t=1-\frac{CD_t}{CB_t}$；$CR_t$ 为引入 $\delta D_t|SD_t|$ 之后获得的签收信度，即 $CR_t=CR'_t+\delta D_t|SD_t|$，对应签收距离 $CD_t=|CR_t-CB_t|$，签收信度逼近度为 $DACR_t=1-\frac{CD_t}{CB_t}$。

如图 2(a)所示，当签收行为呈现突发恶化趋势时有 $D_t<0$ 且 $SD_t<0$，由于 $0<\delta<1$ 有 $\delta D_t|SD_t|<0$，进而有 $|CR'_t-CB_t+\delta D_t|SD_t||<|CR'_t-CB_t|$，依据定义 6 有 $CD_t<CD'_t$，由定义 7 有 $DACR'_t<DACR_t$。

如图 2(b)~图 2(d)所示，当恶意签收行为呈现持久化趋势($D_t\leqslant 0$，$SD_t\geqslant 0$)、签收行为呈现突发改善趋势($D_t>0$，$SD_t>0$)、诚实签收行为呈现持久化趋势($D_t\geqslant 0$，$SD_t\leqslant 0$)时证明类似。证毕。

4.4　抑制策略形成

定义 8　签收信度阈值(CRT, certified reputation threshold)特指电邮实体在电邮行为实施过程中所能容忍的对方实体最低签收信度。

抵赖抑制策略的形成使用了基于签收信度阈值的比较方法。具体思路为：在电邮收发方签收信度不小于全系统签收信度阈值 $CRT_t(global)$的前提下，若电邮发送方 A 的签收信度 $TV_t(A)$低于电邮接收方 B_i 的签收信度阈值 $CRT_t(B_i)$，则禁止发送，反之则允许发送；若 B_i 签收信度 $TV_t(B_i)$低于 A 的签收信度阈值 $CRT_t(A)$，则禁止接收，反之则允许接收。其合理性可在电邮实体签收行为空间内予以解释：以第一种情况为例，由于 $TV_t(A)$小于 $CRT_t(B_i)$，即 A 在先前签收行为上的综合诚信表现低于 B_i 的承受底限，依据组织行为学的归因论，可以预测到 A 在未来极小时间内大幅度改善签收行为的可能性会极低，为此可禁止 A 向 B_i 发送电邮。

算法 3 给出了抵赖抑制策略形成算法，其中，A 和 $B=\{B_1, B_2,\cdots, B_{|B|}\}$分别为电邮发送方和电邮接收方，$TV_t(x)$和 $CRT_t(x)$分别为电邮实体 x 在 t 轮的签收信度和签收信度阈值。

算法 3　*ISF* // 抑制策略形成算法

输入　$TV_t(A)$, $CRT_t(A)$, $\{TV_t(B_i)\}$,$\{CRT_t(B_i)\}$, $CRT_t(global)$

输出　*ris* // 抵赖抑制策略，元素$(00)_{bit}$为允许交互，$(01)_{bit}$为允许发送禁止接收，$(10)_{bit}$为禁止发送允许接收，$(11)_{bit}$为禁止交互

① $ris\leftarrow\varnothing$;

② for each $B_i\in B$ do {

③　if $TV_t(B_i) < CRT_t(global)$ and $TV_t(A) < CRT_t(global)$ then $ris_i\leftarrow(11)_{bit}$

④　else if $TV_t(A)\geqslant CRT_t(B_i)$ and $TV_t(B_i)\geqslant CRT_t(A)$ then $ris_i\leftarrow(00)_{bit}$

⑤　else if $TV_t(A)\geqslant CRT_t(B_i)$ then $ris_i\leftarrow(01)_{bit}$

⑥　else if $TV_t(B_i)\geqslant CRT_t(A)$ then $ris_i\leftarrow(10)_{bit}$

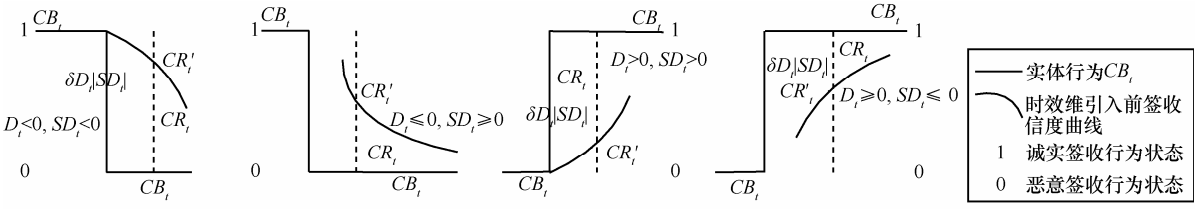
⑦　else　$ris\leftarrow ris\cup ris_i$; }

⑧ return *ris*

5　实验与分析

5.1　实验系统构建

利用 SDN 开源平台构建出如图 3 所示的实验系统，介绍如下：1) 在 SDN 控制器 PC0(运行 Ubuntu12.04+POX)上部署抵赖抑制单元中除电邮证据绑定之外的所有逻辑，以形成抵赖抑制策略；2) 在 OpenFlow 交换机 PC1、PC2(运行 Ubuntu12.04+OpenFlow)上部署定制的流表更新逻辑，以便能够依据抵赖抑制策略更新流表；3) 在 PC3(运行 Win7)上部署定制软件 NRMail，该软件除实现 SMTP 和 POP3 电邮客户端逻辑外，还实现电邮行为提取及证据绑定逻辑（证据绑定时所需的 *TTP* 角色由定制的 *TTP* 进程实现、证据签名及验证由定制的 sign 进程实现）；4) 在 PC4(运行 Win7)上部署共享软件 Winmail 以提供 SMTP 和 POP3 电邮服务。该实验系统中网络 192.168.100.0 中的 PC0、PC1 和 PC2 共同构成电邮控制通道，网络



(a)签收行为呈现突发恶化　(b)恶意签收行为呈现持久化　(c)签收行为呈现突发改善　(d)诚实签收行为呈现持久化

图 2　签收行为 4 类变化原子趋势

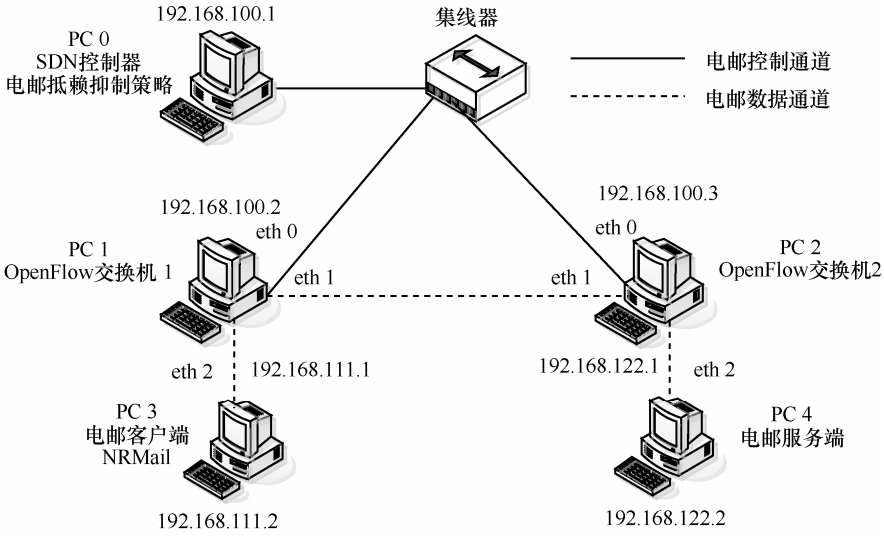


图 3 实验平台

192.168.111.0 中的 PC3、PC1 和 192.168.122.0 网络中的 PC2、PC4 共同构成电邮数据通道。

该实验系统的时序运行过程为：1) NRMail 截获电邮发送的 SOCKET 通信，将所绑定的电邮发送行为证据连同 SOCKET 信息一并提交给 OpenFlow 交换机；2) OpenFlow 交换机缓存该 SOCKET，并将从中解析出的电邮收发方标识与电邮证据(封装成 packet-in 消息)一并通过安全通道(遵守 OpenFlow 协议)直接转发给 SDN 控制器；3) SDN 控制器提取电邮收发方签收信度并据此形成电邮抵赖抑制策略，其结果通过安全通道派发给 OpenFlow 交换机；4) OpenFlow 交换机依据获得的抵赖抑制策略更新流表，在转发本轮后续电邮数据的同时持续向 SDN 控制器提交来自 NRMail 的后续电邮证据；5) SDN 控制器对本轮电邮交互实施抵赖检测，并完成签收信度更新。

5.2 抵赖抑制实验

5.2.1 实验参数选择

1) 电邮实体总数为 1 025（恶意实体占 20%）。同时规定诚实实体诚实宣称真实电邮行为、无共谋（即不会彼此哄抬签收信度）、无诽谤（即不会诋毁他人签收信度）；恶意实体为谋取私利对真实行为会策略地选择诚实宣称或拒绝承认、会共谋抵赖、会对诚实实体实施诽谤。

2) 签收行为注入模型如图 4 所示，同时设置电邮抵赖的行为表现值为 0.1、非抵赖的行为表现值为 1；恶意行为策略时隙为 10 个时间片，即波动周期为 20 个时间片。

3) 签收信度初估时标记抵赖评估证据样本值为 0.1、标记非抵赖样本值为 1，信度合计选用加权简单求和经典算法[23]。

4) 设置签收信度重估参数分别为：α=0.2, β=0.8, γ_1=0.05, γ_2=0.2, δ_1=0.05, δ_2=0.2, ρ=0.75 或 1, LH=10, θ=0.75 或 1, LDH=10。

5) 设置 $CRT_t(global)$=0.4，设置阈值系数为 0.8，即 $CRT_t(x)$= $0.8TV_t(x)$。

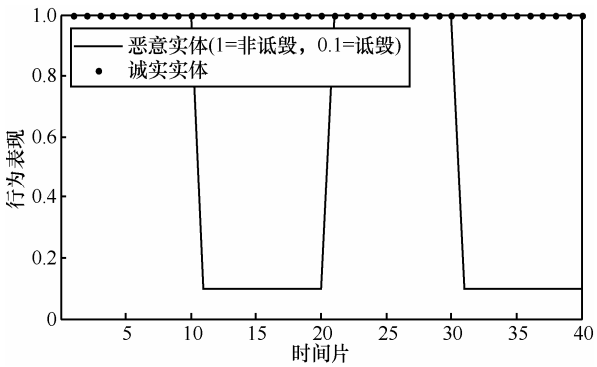


图 4 签收行为注入模型

5.2.2 签收信度逼近测试

签收信度越逼近于签收行为，抵赖抑制策略就越具备针对性。然而，信度类评估所固有的时滞性却会加大签收信度的偏离性。为考查本文方法的签收信度逼近性，以图 4 中行为模型为输入，图 5(a)给出了无共谋情境下，未被诽谤和被诽谤时诚实实体签收信度评估情况，以及 ρ=1 且 θ=1、ρ=1 且 θ=0.75、ρ=0.75 且 θ=1 和 ρ=0.75 且 θ=0.75 时恶意实体签收，与此对应，图 5(b)给出了共谋情境下的

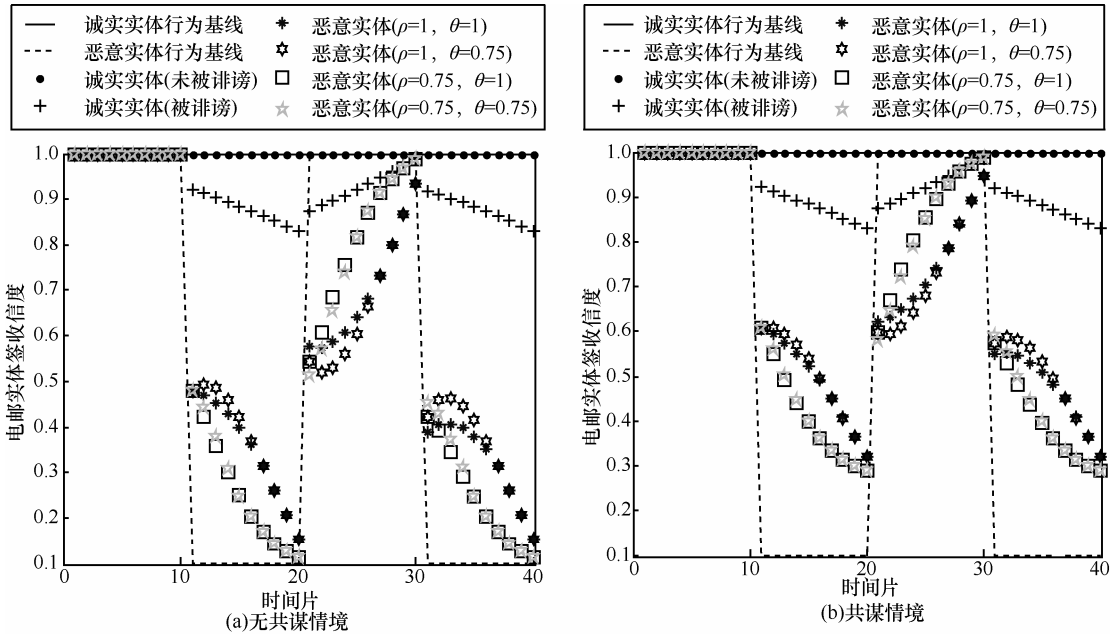


图 5　签收信度评估结果

签收信度评估情况。可以看出：1) 诽谤会降低（诚实实体）签收信度逼近性；2) 虽然共谋会抬升(恶意实体)签收信度，但适当降低 ρ(ρ=0.75<1)和抬升 θ(θ=1>0.75)均可改善签收信度逼近性。

为考查共谋对签收信度逼近性的影响幅度，图 6 针对 ρ=1 且 θ=1、ρ=1 且 θ=0.75、ρ=0.75 且 θ=1 和 ρ=0.75 且 θ=0.75 这 4 组条件，比对了恶意实体在共谋和无共谋时的签收信度评估情况。可以看出，较无共谋而言，当签收行为由诚实转为抵赖时，共谋会加大签收信度偏离性；反之，当签收行为由抵赖转为诚实时，共谋会提升签收信度逼近性。这意味着，恶意电邮实体为更好地隐蔽自身的抵赖行

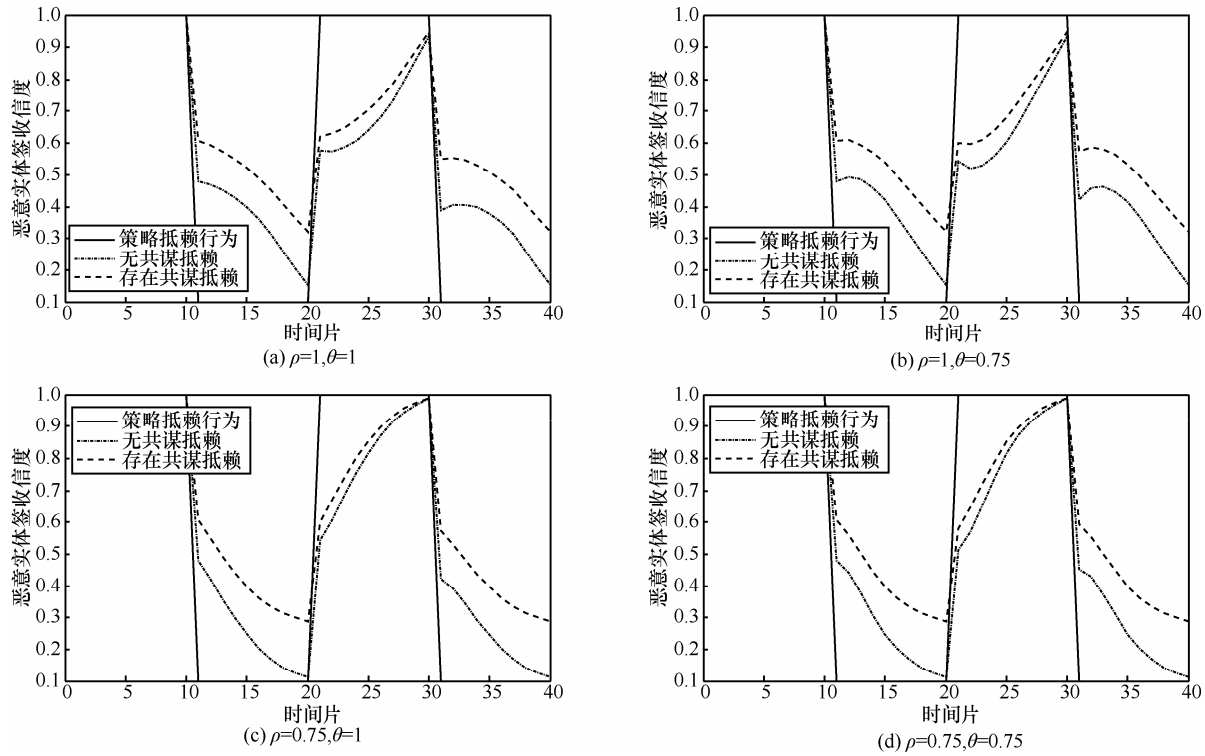


图 6　共谋对逼近性影响幅度分析

为，在试图抵赖电邮行为时会选择共谋，反之，在试图诚实宣称电邮行为时会选择无共谋。

5.2.3 *源头抑制效果检测*

为检测电邮抵赖源头抑制效果，针对无共谋无诽谤、无共谋有诽谤、有共谋无诽谤、有共谋有诽谤 4 种交叉场景（下文简称 4 种交叉场景），图 7 给出了设定 ρ=1，θ=0.75(即签收信度逼近度最差情形)时电邮交互总量逐步增长至 10 000 时被源头抑制掉的电邮发送抵赖、电邮接收抵赖、电邮收发抵赖，以及电邮交互无抵赖这 4 类抵赖情况的占比数据。如表 1 所示，随着电邮交互次数的不断增多，被源头抑制掉的电邮发送抵赖平均占比从最初的 0.243 8 下降（使用"↘"标记）到 0.019 7，电邮接收抵赖平均占比从最初的 0.215 2 下降到 0.019 9，电邮收发抵赖平均占比从最初的 0.013 9 下降到 0，与此同时，电邮交互成功平均占比从最初的 0.620 4 上升（使用"↗"标记）到 0.957 4。这表明，本文提出的电邮抵赖源头抑制方法能够促使电邮实体执行诚信无抵赖的电邮交互。

5.2.4 *源头抑制能力评估*

对电邮抵赖源头抑制能力的评估拟采用 3 种常用的评估分类器度量标准：查全率、查准率和调和平均值。具体地，设 TP 是事前被正确识别为电邮抵赖的样本数、FN 是事前被误判为电邮无抵赖的样本数、FP 是事前被误判为电邮抵赖的样本数，则电邮抵赖查全率 $R=\frac{TP}{TP+FN}$、电邮抵赖查准率 $P=\frac{TP}{TP+FP}$、调和平均值 $F=2P\frac{R}{P+R}$。

针对 4 种交叉场景，图 8 给出了 ρ=1，θ=0.75 时电邮交互总量从 1 增长到 10 000 时的电邮抵赖查全率、电邮抵赖查准率和调和平均值。从表 2 可以看出，虽然在 4 种交叉场景下的电邮抵赖查全率均值仅为 0.373 0，但查准率却高达 0.999 2，并且还

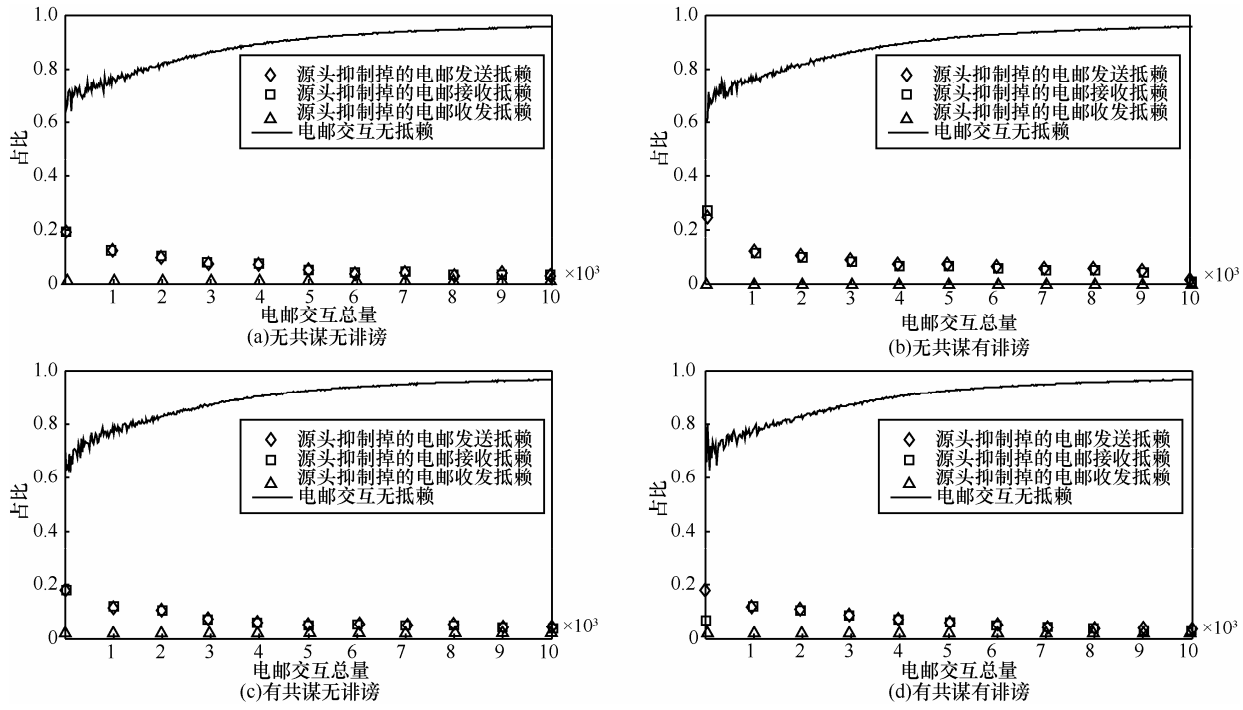


图 7　电邮抵赖源头抑制实验结果

表 1　　**电邮抵赖源头抑制效果分析**

类型	无共谋无诽谤	无共谋有诽谤	有共谋无诽谤	有共谋有诽谤	均值
发送抵赖	0.250 0↘0.020 0	0.250 0↘0.019 0	0.250 0↘0.020 2	0.225 0↘0.019 6	0.243 8↘0.019 7
接收抵赖	0.233 3↘0.020 1	0.200 0↘0.019 0	0.177 3↘0.020 4	0.250 0↘0.020 2	0.215 2↘0.019 9
收发抵赖	0.016 7↘0	0.023 1↘0	0.010 0↘0	0.005 6↘0	0.013 9↘0
无 抵 赖	0.616 7↗0.957 7	0.610 0↗0.957 5	0.630 0↗0.957 2	0.625 0↗0.957 2	0.620 4↗0.957 4

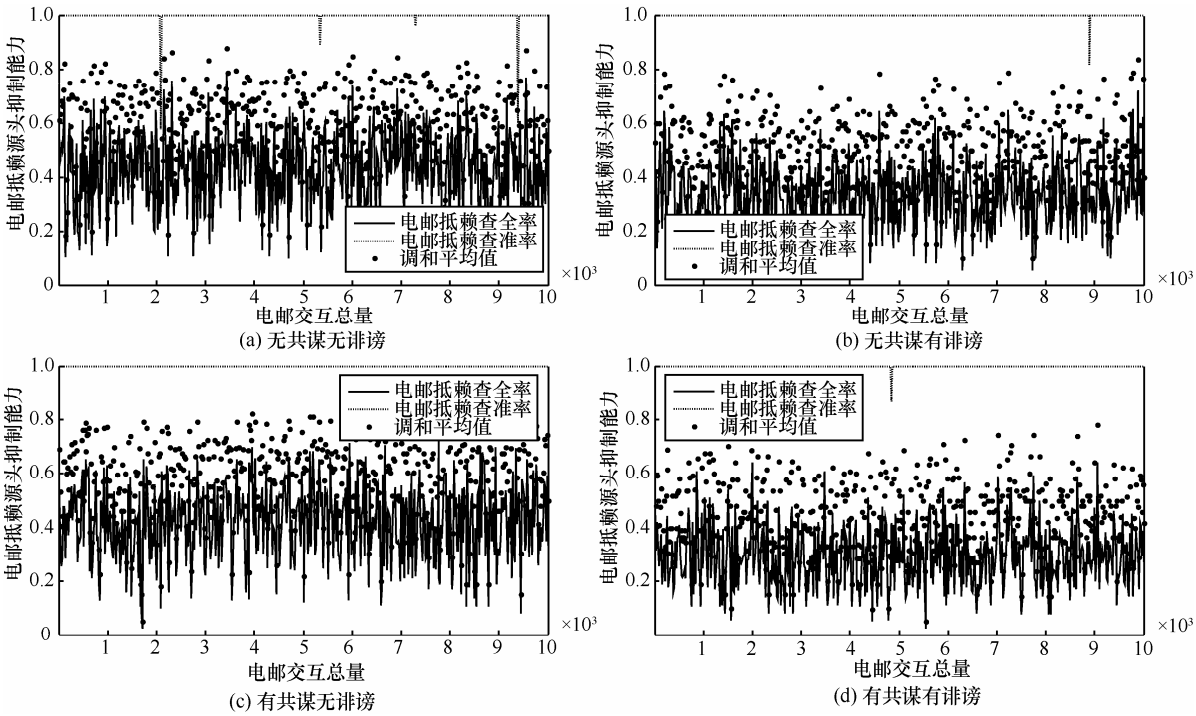


图 8　电邮抵赖查全率、查准率和调和平均值

表 2　　**电邮抵赖源头抑制能力分析**

类型	无共谋无诽谤		无共谋有诽谤		有共谋无诽谤		有共谋有诽谤		平均
	区间	均值	区间	均值	区间	均值	区间	均值	
抵赖查全率	[0.025 6, 0.812 5]	0.434 8	[0.052 6, 0.720 9]	0.334 8	[0.052 6, 0.766 7]	0.434 9	[0.050 0, 0.625 0]	0.287 4	0.373 0
抵赖查准率	[0.875 0, 1]	0.998 1	[0.818 2,1]	0.999 6	[0.702 7, 1]	0.999 1	[0.947 4,1]	0.999 9	0.999 2
调和平均值	[0.050 0, 0.896 6]	0.592 5	[0.100 0, 0.837 8]	0.490 1	[0.095 2, 0.867 9]	0.587 8	[0.095 2, 0.769 2]	0.435 0	0.526 4

获得了 0.526 4 的较好调和平均值，这表明本文方法具备一定的电邮抵赖源头抑制能力。

5.2.5　与签收电邮的比较

为确保比较的公平性，通过裁剪 5.1 节的实验系统构建出待比较的签收电邮系统，即切断图 3 中的 PC0，修改 PC1、PC2 上流表以双向允许 PC3、PC4 间的分组，保留 PC3 上的 NRMail 和 PC4 上的电邮服务。

图 9 给出了 ρ=1，θ=0.75 时电邮交互总量从 1 增长到 10 000 时，本文方法与签收电邮的电邮抵赖抑制对比情况。从表 3 和表 4 可以看出，在同种系统配置下，当电邮交互总量达到 10 000 时，4 种交叉场景下本文方法的电邮抵赖源头抑制的占比与签收电邮的电邮抵赖事后抑制占比相当，分别达到了 94.85%、99.53%、99.09%和 99.10%，这表明本文方法有效弥补了签收电邮在抵赖源头抑制上的不足。

6　结束语

基于 SDN 技术，提出一种不破坏现有电邮结构的电邮抵赖源头抑制方法，解决了现有以签收电邮为代表的电邮安全技术仅能对电邮抵赖进行事后检测而无法实施源头抑制的问题。考虑到本文方法在电邮抵赖查全率上还有提升空间，下一步工作拟分 2 步进行：1) 设计出抵赖危害评估模型，以对电邮抵赖的危害性进行界定；2) 基于电邮通联网络提出电邮抵赖传播与扩散机制，以获取危害性电邮抵赖的行为态势。在改善电邮抵赖源头抑制针对性的同时，通过扩大电邮抵赖的预测面来提升电邮抵赖的源头查全率。

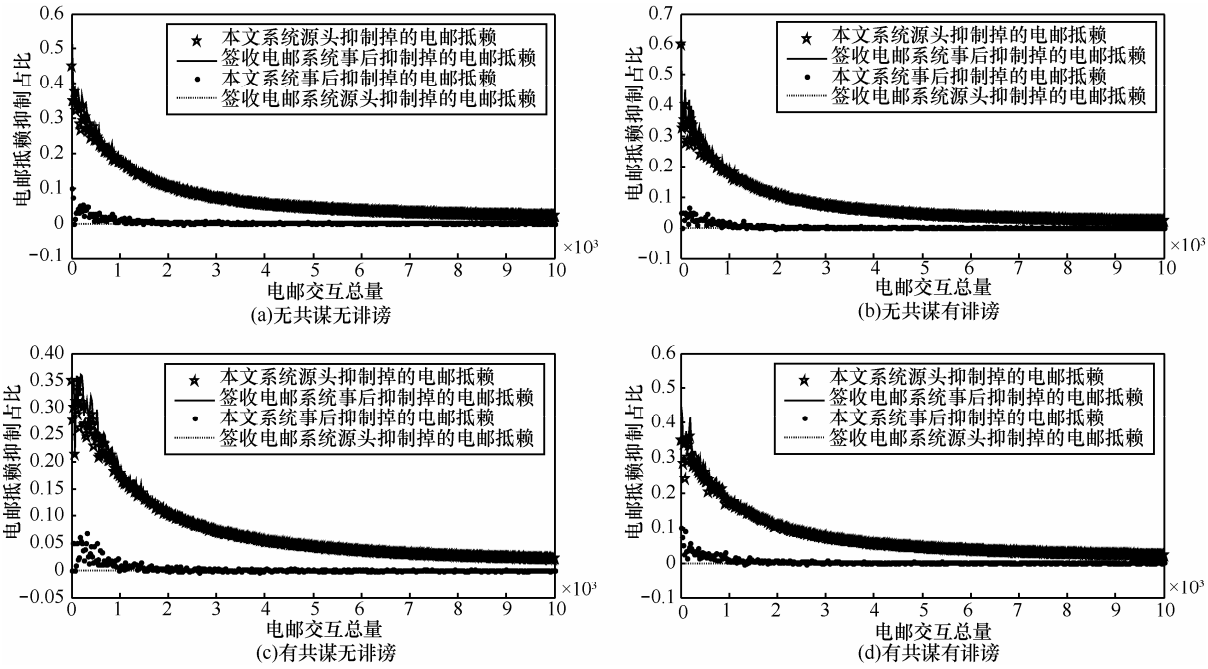


图 9　源头抑制与事后抑制实验结果

表 3　　**无共谋情境下抵赖抑制占比（抑制数/交互量）**

抵赖抑制类别		无共谋无诽谤下交互总量					无共谋有诽谤下交互总量				
		100	500	1 000	2 000	10 000	100	500	1 000	2 000	10 000
源头抑制	本文	0.380 0	0.250 0	0.185 0	0.108 5	0.022 1	0.270 0	0.256 0	0.184 0	0.104 0	0.021 2
	签邮	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
事后抑制	本文	0.020 0	0.022 0	0.015 0	0.003 5	0.001 2	0.050 0	0.012 0	0.007 0	0.006 0	0.000 1
	签邮	0.400 0	0.272 0	0.200 0	0.112 0	0.023 3	0.320 0	0.268 0	0.191 0	0.110 0	0.021 3
本文源头/签邮事后		95.00%	91.91%	92.5%	96.88%	94.85%	84.38%	95.52%	96.34%	94.55%	99.53%

表 4　　**有共谋情境下抵赖抑制占比（抑制数/交互量）**

抵赖抑制类别		有共谋无诽谤下交互总量					有共谋有诽谤下交互总量				
		100	500	1 000	2 000	10 000	100	500	1 000	2 000	10 000
源头抑制	本文	0.290 0	0.232 0	0.180 0	0.106 0	0.021 7	0.240 0	0.260 0	0.176 0	0.109 0	0.021 9
	签邮	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
事后抑制	本文	0.120 0	0.034 0	0.004 0	0.003 0	0.000 2	0.050 0	0.026 0	0.011 0	0.002 5	0.000 2
	签邮	0.410 0	0.266 0	0.184 0	0.109 0	0.021 9	0.290 0	0.286 0	0.187 0	0.111 5	0.022 1
本文源头/签邮事后		70.73%	87.22%	97.83%	97.25%	99.09%	82.76%	90.91%	94.12%	97.76%	99.10%

参考文献：

[1] WELLS T M, DENNIS A R. To e-mail or not to e-mail: the impact of media on psychophysiological responses and emotional content in utilitarian and romantic communication[J]. Computers in Human Behavior, 2016, 54: 1-9.

[2] TAUBER A. A survey of certified mail systems provided on the Internet[J]. Computers & Security, 2011, 30: 464-485.

[3] FERRER-GOMILLA J L, ONIEVA J A, PAYERAS M, et al. Certified electronic mail: properties revisited [J]. Computers & Security, 2010, 29(2):167-179.

[4] KIM H, FEAMSTER N. Improving network management with software defined networking [J]. IEEE Communications Magazine, 2013, 51(2):114-119.

[5] ALI S T, SIVARAMAN V, RADFORD A, et al. A survey of securing networks using software defined networking [J]. IEEE Transactions on Reliability, 2015,64(3): 1086-1097.

[6] BECHTOLD S, PERRIG A. Accountability in future Internet architectures[J]. Communications of the ACM, 2014, 57(9): 21-23.

[7] WANG Y, SUSILO W, AU MH, et al. Collusion-resistance in optimistic fair exchange[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(8):1227-1239.

[8] ONIEVA J A, ZHOU J, LOPEZ J. Enhancing certified e-mail service for timeliness and multicast[C]// 2004 International Network Conference. Plymouth, UK, 2004: 327-336.

[9] MICALI S. Simple and fast optimistic protocols for fair electronic exchange[C]//The twenty-second annual symposium on Principles of distributed computing. Boston, USA, 2003: 12-19.

[10] SHAO MH, WANG G, ZHOU J. Some common attacks against certified e-mail protocols and the countermeasures[J]. Computer Communications, 2006, 29(15): 2759-2769.

[11] PAYERAS-CAPELLÀ M M, MUT-PUIGSERVER M, FERRER-GOMILA J L, et al. No author based selective receipt in an efficient certified e-mail protocol[C]//2009 17th Euromicro International Conference on Parallel, Distributed and Network-based Processing. Weimar, 2009:387-392.

[12] PUIGSERVER M M, GOMILA J L F, ROTGER L H. Certified electronic mail protocol resistant to a minority of malicious third parties[C]//Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM 2000). 2000: 1401-1405.

[13] ATENIESE G, MEDEIROS BD, GOODRICH MT. TRICERT: a distributed certified e-mail schemes[C]//2001 Network and Distributed System Security Symposium. San Diego, USA, 2001.

[14] ZHOU J, ONIEVA J, LOPEZ J. Optimized multi-party certified e-mail protocols[J]. Information Management & Computer Security, 2005, 13(5):350-366.

[15] WANG C, LAN C, NIU S, et al. An ID-based certified e-mail protocol with STTP suitable for wireless mobile environments[J]. Journal of Computers, 2013,8(1): 3-9.

[16] TAUBER A, APITZSCH J, BOLDRIN L. An interoperability standard for certified mail systems[J]. Computer Standards & Interfaces, 2012, 34: 452-466.

[17] TAUBER A, KUSTOR P, KARNING B. Cross-border certified electronic mailing: a European perspective[J]. Computer Law & Security Review, 2013, 29(1):28-39.

[18] DRAPER-GIL G, FERRER-GOMILA JL, HINAREJOS MF, et al. An optimistic certified e-mail protocol for the current Internet e-mail architecture[C]//2014 IEEE Conference on Communications and Network Security(CNS). San Francisco, 2014: 382-390.

[19] PAULIN A, WELZER T. A universal system for fair non-repudiable certified e-mail without a trusted third party [J]. Computers & Security, 2013,32: 207-218.

[20] LARA A, KOLASANI A, Ramamurthy B. Network innovation using OpenFlow: a survey [J]. IEEE Communications Surveys & Tutorials, 2014, 16(1): 493-512.

[21] KREUTZ D, RAMOS F M V, VERISSIMO P E, et al. Software-defined networking: A comprehensive survey[J]. Proceedings of the IEEE, 2015,103(1): 14-76.

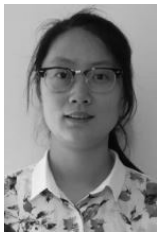
[22] SYVERSON P, VAN OORSCHOT P C. A unified cryptographic protocol logic[R]. Technical Report, NRL Publication 5540-227, Naval Research Lab, 1996.

[23] HENDRIKX F, BUBENDORFER K, CHARD R. Reputation systems: A survey and taxonomy [J]. Journal of Parallel and Distributed Computing, 2015, 75: 184-197.

[24] SRIVATSA M, XIONG L, LIU L. TrustGuard: countering vulnerabilities in reputation management for decentralized overlay networks[C]//The 14th international conference on World Wide Web (WWW2005). Chiba, Japan, 2005.

作者简介：

韩志耕（1976-），男，江苏东台人，博士，南京审计大学讲师，主要研究方向为网络安全与管理。



冯霞（1983-），女，江苏扬中人，安徽大学博士生，主要研究方向为数据安全。

陈耿（1965-），男，江苏无锡人，博士，南京审计大学教授、硕士生导师，主要研究方向为数据安全、网络取证。