

# 基于匿名通信的在线匿名秘密举报方案

杨 阳<sup>1,2</sup>, 李晓宇<sup>1</sup>

(1. 郑州大学 信息工程学院, 郑州 450001; 2. 天津市和平区网格化管理中心, 天津 300041)

**摘 要:** 为保护举报者的身份隐私(身份信息和位置信息)不被包含举报受理机构在内的任意组织获取,提出一种在线匿名秘密举报方案。匿名举报者借助公开密钥算法通过随机转发的方法将加密举报信息发送给举报受理机构,加密举报信息经过网络中一系列中转节点的转发最终到达举报受理机构,任何中转节点和攻击者不能获取举报信息的明文,包含举报受理机构在内的所有节点以及外来攻击者无法取得举报人的身份隐私,如举报信息属实,举报机构可以对举报者进行奖励,同时仍然保持举报者的身份和位置信息不会泄露给举报受理机构或者任意第三方。由于中转节点是随机选择的,不依赖于某些特定节点,从而保证系统的健壮性。实验结果表明,该方案能够支持大型网络中多个举报者顺利完成举报,系统不会出现平均响应时间随节点个数增加而急剧增长的现象,具有良好的可靠性和稳定性。

**关键词:** 匿名秘密举报;匿名通信;公开密钥系统;随机转发;身份隐私

开放科学(资源服务)标志码(OSID):



中文引用格式:杨阳,李晓宇.基于匿名通信的在线匿名秘密举报方案[J].计算机工程,2022,48(5):118-126.

英文引用格式:YANG Y, LI X Y. Online anonymous whistleblowing scheme based on anonymous communication[J]. Computer Engineering, 2022, 48(5): 118-126.

## Online Anonymous Whistleblowing Scheme Based on Anonymous Communication

YANG Yang<sup>1,2</sup>, LI Xiaoyu<sup>1</sup>

(1. School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China;

2. Tianjin Heping District Grid Management Center, Tianjin 300041, China)

**[Abstract]** In order to protect the whistleblower's identity privacy (identity information and location information) from being acquired by any organization, including the one that the whistleblower reports to, an online secret whistleblowing scheme is proposed. The scheme allows the anonymous whistleblower to send encrypted messages to the target agency by using a public key algorithm and a random forwarding method. The encrypted messages are forwarded for several times by a sequence of nodes in the network, and finally reach the target agency. Any forwarding node or attacker cannot get the plaintext of the original message, nor could any node, including the target agency or any third party, get the identity privacy of the whistleblower. If the reported information is verified, the target agency can award the whistleblower while the identity and location information of the whistleblower remains undisclosed. In addition, all forward nodes are randomly chosen and the proposed scheme doesn't rely on any specific node, so the robustness of the system is ensured. Experimental results show that the proposed scheme can support multiple whistleblowers to report messages in a large-scale network while the average response time does not grow sharply with the number of nodes, so the system displays high reliability and stability.

**[Key words]** anonymous secret whistleblowing; anonymous communication; public key system; random forwarding; identity privacy

DOI: 10.19678/j.issn.1000-3428.0060755

### 0 概述

随着互联网技术的快速发展,用户在使用网络通信的过程中对自身隐私信息的保护意识不断增

强。在用户使用网络进行举报的过程中,如何进行安全举报、保障举报人的隐私等安全问题日益凸显,成为人们关注的重点之一。当前,主流的加密技术是通过通过对信息进行加密的方式,使得信息内容能够

基金项目:国家自然科学基金(61876016)。

作者简介:杨 阳(1994—),女,硕士,主研方向为移动信息安全、匿名通信;李晓宇(通信作者),副教授、博士。

收稿日期:2021-02-01 修回日期:2021-05-23 E-mail: icxyli@zzu.edu.cn

得到有效隐藏,从而保护了网络传输过程中信息内容的安全性,但是信息的发送者和接收者的相关信息,如身份、位置等隐私信息却不能被隐藏。在网络举报过程中要想实现对发送节点身份和位置信息的保护,可将匿名通信技术应用并贯穿到用户的整个举报过程中。

匿名通信<sup>[1]</sup>是指采用一定的方法将网络通信中的节点身份信息和通信关系进行隐藏,使得攻击者无法通过分析流量或窃听的方式来倒推出节点间的关系,并无法追踪到节点的通信过程,从而实现通信节点身份信息和位置信息的保密性和安全性。文献[2]提出一种匿名通信技术,即 Mix 技术,该技术通过采用随机选择、固定转发策略完成通信重路由路径的建立,从而使窃听者无法获取消息的传输路径。为实现移动通信中位置的隐私保护。为实现移动通信中位置的隐私保护,文献[3]基于空间混淆提出一种位置隐私保护方法,并提出位置隐私区域的生成算法,但该算法在需要提供高质量通信服务时,位置的模糊程度被限制,因而不能有效地保护位置信息隐私保护。文献[4]提出一种基于差分扰动的均衡增量近邻查询方法来实现隐私保护。该方法通过将可控的拉普拉斯噪声添加到用户的真实位置中,并生成干扰位置,再将干扰位置作为锚点,发送给位置服务商,这样用户的隐私性便得到了保证。文献[5-7]介绍了其他一些匿名通信方案。

在线匿名举报是有效保护举报人身份的一个重要途径,被举报人甚至举报受理机构都不可能获取举报人身份,从而消除举报人的后顾之忧,鼓励大家积极举报,是反腐败、反渎职和反商业犯罪的威力强大的手段。文献[8]提出一种支持悬赏的匿名举报方案,文献[9]对该方案的安全性进行了分析并给出系统设计框架。文献[10]提出一种基于比特承诺的可撤销的匿名电子检举方案。文献[11]提出一种利用基于身份的密码体制的匿名电子举报方案。文献[12-14]提出一些匿名举报方案并且对其在现实中的应用进行分析。

上述匿名举报方案主要着眼于保证举报者在发送举报消息过程中不泄露身份信息,但是没有考虑到现实中举报受理机构(或者其他攻击者)可以通过追踪举报消息的来源而确定举报者的 IP 地址和地理位置,进而通过线下手段获取举报人的身份。为克服上述问题,本文提出一种基于匿名通信技术的匿名秘密举报方案。用户使用匿名通信技术将举报信息发送给服务器,保证用户的身份和位置信息不会被包括举报受理机构在内的任意个人或者机构获取,且举报信息绝对保密,只有举报受理机构可以读取。该方案所有用户所在的终端都加入到网络中并以对应的节点表示,在整个通信过程中采用混合加密技术<sup>[5]</sup>加密消息、随机选择节点转发消息的策略

来实现通信过程的匿名性和举报消息的保密性,通过使用随机的转发路径来防止流量分析和追踪攻击。

## 1 匿名秘密举报方案

为实现匿名秘密举报,本文主要采取了以下3个技术要点:1)使用匿名通信算法通过中转节点来进行消息的转发,实现了对举报人身份、位置信息、举报内容等隐私的保护;2)举报方案依赖于公开密钥系统,但是公开密钥算法的加密/解密效率相对较低,使用举报受理机构的公开密钥直接来加密举报内容(可能是大量的数据)是不合适的,因此,采用混合加密技术用对称密钥算法对明文消息进行加密解密操作,用公开密钥对所用到的对称密钥进行加密解密操作,从而保证了这些举报信息的安全可靠、不可泄露和不可伪造等特性;3)设计一种具有奖励机制的举报方案,以鼓励用户举报。

匿名秘密举报方案的基本思路是举报人采用匿名通信机制向举报受理机构发出举报信息,除举报受理机构外,其他任何人都不能获得举报信息的内容,并且任何人包括举报受理机构都无法获知发送举报人的身份和位置信息<sup>[15-17]</sup>。匿名举报方案可以使举报人能够完全隐藏自己的身份及位置信息,以防遭到别人的恶意报复。若举报内容被证明属实,举报受理机构会给予举报人奖励,在奖励过程中,同样采用匿名通信机制实现对举报人身份信息和位置信息的保密,确保这些信息不会被任何人包括举报受理机构获得。同时,举报受理机构能够核实举报信息确实来自举报人,并对真正的举报人进行奖励,任何人不能假冒举报人领奖。

### 1.1 匿名通信协议

在初始时网络中所有节点(含举报受理机构的服务器)加入到一个 RSA 公开密钥系统中。作为公开密钥系统的成员,各个节点使用 RSA 算法生成一对密钥:一个私有密钥  $Sk_i$  和一个公开密钥  $PK_i$ 。所有节点的私有密钥自己绝对保密,而公开密钥都保存在密钥管理中心,节点通过 ID 号查询密钥管理中心便可以获得其他节点的公开密钥。此外,服务器的身份和位置是公开的,而其他节点真实身份和位置则是保密的。

当发送节点采用匿名通信协议向服务器发送消息时主要有以下3个步骤:

1)先加密消息。采用对称加密和非对称加密的混合加密来完成对消息的加密操作。

2)转发加密后的消息。利用随机选择的中转节点进行消息的转发,消息经过多次转发最后到达服务器。因为消息是加密的,所以除服务器外,每一个中转节点都不能获取消息的内容。

3)返回确认的消息。服务器回复发送节点的消息。

息是按照原消息路径进行返回,最后到达发送节点。

这个协议可以确保任意中转节点和服务器的都不知道该消息的发送者是哪个节点,从而保护了发送节点的身份和位置隐私,真正实现了匿名通信。匿名通信模型如图1所示。

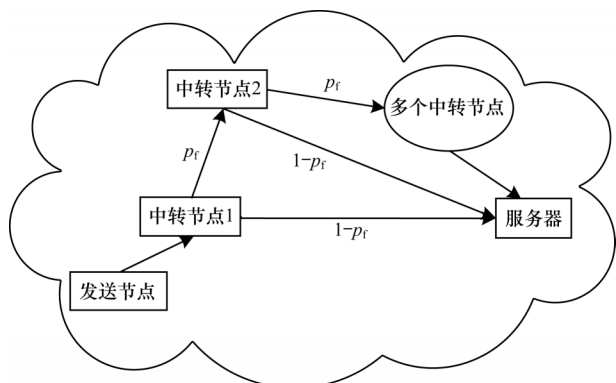


图1 匿名通信模型

Fig.1 Anonymous communication model

在本文方案中,每一个中转节点接收到消息再转发都是一个抽出举报信息(密文)后重新选择转发目标的过程,是在应用层实现的,所以是一次新的通信过程。因此,通过发路由表、源地址、目的地址等方法实现溯源最多只能溯源到上一个转发节点,不可能找到最初的发送者。

#### 1.1.1 发送节点发送消息过程

发送节点将要发送的消息记作 $P$ ,并为该消息生成序列码 $s$ ,该序列码随机产生。

首先发送节点 $r_0$ 用AES算法生成两个对称密钥 $K_0$ 和 $K_1$ 。 $K_0$ 用于对消息 $P$ 进行加密,形成密文 $m$ ,用服务器的公开密钥 $PK_s$ 加密对称密钥 $K_0$ ,将这两者与序列码 $s$ 组合在一起形成报文 $m_k$ 。发送节点 $r_0$ 用对称密钥 $K_1$ 对报文进行加密,作为发送消息的第1个部分。发送节点 $r_0$ 随机选择下一个节点 $r_1$ , $r_1$ 是不同于服务器和 $r_0$ 的其他中转节点。然后用第1个中转节点 $r_1$ 的公开密钥 $PK_1$ 对密钥 $K_1$ 进行加密,形成发送消息的第2个部分。将这2个部分组合起来,便可得到发送节点 $r_0$ 最终要发送的消息。

#### 算法1 发送节点发送消息算法

1. 用AES算法为发送节点 $r_0$ 生成密钥 $K_0$ 和 $K_1$ ;
2. 发送节点 $r_0$ 通过ID号在密钥管理中心查询到服务器的公开密钥 $PK_s$ ;
3.  $m = E_{K_0}(P)$ ; //用对称密钥 $K_0$ 对消息 $P$ 加密
4.  $m_1 = E_{PK_s}(K_0)$ ; //用服务器的公开密钥 $PK_s$ 加密对称密钥 $K_0$
5.  $c_1 = E_{K_1}(m, m_1, s)$ ; //用对称密钥 $K_1$ 对 $m, m_1, s$ 的组合成的报文 $m_k$ 进行加密
6.  $c_2 = E_{PK_1}(K_1)$ ; //用第一个中转节点 $r_1$ 的公开密钥 $PK_1$ 对密钥 $K_1$ 进行加密
7. 发送消息  $SEND_{r_0} = (c_1, c_2)$ 。

#### 1.1.2 中转节点转发消息过程

发送节点 $r_0$ 将消息先发送给中转节点 $r_1$ 。当节点 $r_1$ 收到消息后,先用节点 $r_1$ 的私有密钥 $SK_1$ 对消息的第2部分 $c_2$ 进行解密操作,得到对称密钥 $K_1$ ,再用 $K_1$ 解密消息的第1部分 $c_1$ ,得到报文,并将序列号 $s$ 和发送节点 $r_0$ 的IP地址存入到路由表 $t_i$ 中,如表1所示(所有节点 $i$ 都有一个相对应的表格 $t_i$ ),并对路由表进行更新。最后中转节点 $r_1$ 以概率 $p_f$ 发给服务器,或者以概率 $1-p_f$ 发给除 $r_1$ 和 $r_0$ 之外的节点中随机选出的中转节点 $r_2$ 。

表1 路由表

Table 1 Routing table

序列码	上一个节点IP
S1	IP1
S2	IP2
⋮	⋮

无论中转节点 $r_i$ 发给除服务器外的哪个节点,都是先用随机选择一个AES对称密钥 $K_i$ 对报文进行加密,作为消息的第1部分,并用该节点的公开密钥 $PK_{i+1}$ 对密钥 $K_i$ 进行加密,作为消息的第2个部分,然后将这两部分内容组成最终要发送的消息,再进行转发操作。

中转节点 $r_2$ 收到消息后进行和中转节点 $r_1$ 同样的操作,并将记录下的序列号 $s$ 、上一个节点 $r_1$ 的IP地址存入表 $t_2$ 中,同时更新路由表。然后以相同的概率将消息发送给服务器或者中转节点 $r_3$ 。当中转节点 $r_3$ 收到消息之后,重复上述过程。经过多个中转节点的转发操作之后,消息最终到达服务器。

因此,消息不是直接发给服务器,而是经过一组中转节点 $r_1, r_2, \dots, r_k$ 的多次转发,最终被服务器接收到。

#### 算法2 中转节点对消息进行转发算法

1. for( $i=0; i \leq k; i++$ ) {
2. 中转节点 $r_i$ 收到消息;
3.  $D(SEND_{r_0}) = D(c_1, c_2)$ ; //用私有密钥 $SK_1$ 对消解密,得到对称密钥 $K_1$ 、序列号 $s$
4. if(序列号 $s$ 和其对应的发送节点的IP地址存在于表 $t_i$ 中) then
5. 当前节点对报文 $m_k$ 进行加密;
6. 查询路由表 $t_i$ ,选择相匹配的且是最新的一条记录,并用序列号 $s$ 对应节点的对称密钥 $K_{i-1}$ 加密报文 $m_k$ ,公开密钥 $PK_{i-1}$ 加密密钥 $K_{i-1}$ ;
7. 发送给序列号 $s$ 对应的IP地址的中转节点;
8. 将这条最新的记录删除;
9. Break;
10. else
11. 将序列号 $s$ 和上一个节点的IP地址写入路由表 $t_i$ 中;
12. if( $rand() \% 2 == 0$ ) then //判断一个随机数是否是偶数
13. 发送给服务器;



14. 采用当前节点  $r_i$  的对称密钥和服务器的公钥对消息加密;
15. Break;
16. else {
17. 在路由表中将当前节点和上一个中转节点删除;
18. 随机选出一个中转节点, 并用该节点的对称密钥对报文进行加密, 公开密钥加密对称密钥;
19. 转发消息给中转节点  $r_{i+1}$ ;
20. }
21. }

### 1.1.3 服务器发送回复消息过程

如果服务器要回复消息给发送节点, 则执行以下步骤:

1) 服务器根首先据序列号  $s$  找到转发该消息给自己的节点 (即最后一个中转节点), 接着服务器回复发送节点的消息作  $P_1$ , 服务器向中转节点发送的消息记作  $ANS_{r_0}$ , 它由 2 个部分组成: 第 1 个部分是用解密得到的发送节点  $r_0$  的密钥  $K_0$  加密消息  $P_1$ , 产生密文, 然后将原序列码  $s$  和密文组合起来, 用服务器的对称密钥  $K_s$  对组合起来的内容进行加密操作; 第 2 个部分是采用序列码  $s$  所对应节点的公开密钥  $PK_i$  加密服务器的对称密钥  $K_s$ , 利用序列码  $s$  查找简易路由表, 得到转发消息给自己的上一个节点  $r_i$ 。

2) 中转节点  $r_i$  收到服务器发来的消息后, 用私有密钥  $SK_i$  对消息进行解密操作, 得到服务器的对称密钥  $K_s$ , 再用解密得到的  $K_s$  去解密消息的第 1 个部分, 从而得到序列码和密文。用节点的对称密钥  $K_i$  加密序列码和密文, 然后查找路由表  $t_i$ , 选择此消息序列码所对应的节点的公开密钥  $PK_{i-1}$  去加密节点的对称密钥  $K_i$ 。将路由表中查到的 IP 地址发送给节点  $r_{i-1}$ , 同时将表中的该项记录删除。

3) 若中转节点  $r_{i-1}$  接收到消息, 那么重复步骤 2, 继续转发回复消息; 直到消息到达最初的发送节点  $r_0$ 。

4) 发送节点  $r_0$  收到消息后, 用自己的私有密钥  $SK_{r_0}$  对消息进行解密, 从而得到对称密钥  $K_1$ , 再用  $K_1$  继续解密消息, 获得序列码和密文。最后发送节点用自己的密钥  $K_0$  解密密文, 便可得到服务器发送的回复消息  $P_1$ 。

#### 算法 3 服务器发送回复消息算法

1.  $SEND_{r_0} = (c_1, c_2) = (PK_1(s, K_0(P)), PK_s(K_0))$ ; // 服务器收到消息
2.  $D(SEND_{r_0}) = D(PK_1(s, K_0(P)), K_0)$ ; // 服务器使用私钥  $SK_s$  解密  $SEND_{r_0}$ , 得到  $K_0$  和  $s$
3. 将  $s$  和上一个节点的 IP 地址记录到表  $t_s$  中;
4.  $D(K_0(P)) = P$ ; // 服务器用  $K_0$  解密密文
5. 用密钥  $K_0$  对回复消息  $P_1$  进行加密,  $c' = K_0(P_1)$ ;
6.  $ANS_{r_0} = (K_s(s, K_0(P_1)), PK_s(K_s))$ ; // 服务器生成发送消息;
7. if (序列号  $s$  和对应的中转节点的 IP 地址存在于表  $t_i$  中) then
8. 查询路由表  $t_i$ ;

9. 将服务器发送的消息  $ANS_{r_0}$  发送给表中序列号  $s$  对应的 IP 地址的上一个中转节点  $r_i$ ;
10. 发送节点  $r_0$  收到服务器发送的回复消息  $ANS_{r_0}$ ;
11. Break;
12. 发送节点  $r_0$  用私有密钥  $SK_{r_0}$  和对称密钥  $K_0$  进行解密, 获得回复信息  $P_1$ 。

## 1.2 匿名举报方案

举报人利用匿名通信技术实现匿名举报的基本过程如下:

1) 举报人利用匿名通信协议将举报信息发送给举报受理机构。

2) 举报受理机构收到举报信息后, 记录举报信息并且利用匿名通信协议向举报人回复一条确认信息。

3) 举报人收到回复消息, 确认自己的举报已经被受理, 且举报信息未被篡改。

### 1.2.1 举报人举报信息的发送

举报人发送举报信息过程如下:

1) 假定举报人位于节点  $r_0$ , 使用 AES 算法生成密钥  $K_0$ 。举报人作为初始发送节点发送举报信息。发送的举报信息包含两部分内容: 第 1 个部分先生成 AES 密钥  $K_0$  对将要发送的明文举报信息  $P$  进行加密, 形成密文  $c$ ; 第 2 个部分用举报受理机构  $s$  的公开密钥  $PK_s$  对发送节点  $r_0$  的对称密钥  $K_0$  进行加密。

2) 举报人调用匿名通信协议算法将举报信息发送至举报受理机构。

#### 算法 4 举报人发送举报消息算法

1. 举报人使用 AES 算法生成对称密钥  $K_0$  和  $K_1$ ;
2.  $c_1 = E_{K_1}(K_0(P), PK_s(K_0), s)$ ; // 用 AES 和 RSA 算加密 // 举报信息  $P$ 、密钥  $K_0$  和序列号  $s$
3.  $c_2 = E_{PK_1}(K_1)$ ; // 用下一个中转节点  $r_1$  的公开密钥 //  $PK_1$  加密  $K_0$
4. 生成举报人要发送消息  $SEND_{r_0} = (c_1, c_2)$ ;
5. 举报人作为初始发送节点  $r_0$  调用算法 1, 将消息  $SEND_{r_0}$  发送给  $r_1$ ;
6. 中转节点  $r_1$  收到消息  $SEND_{r_0}$  后, 调用算法 2 进行消息的转发操作;
7. 举报受理机构接收到消息  $SEND_{r_0}$ 。

### 1.2.2 举报受理机构确认信息的回复

举报受理机构收到最后一个中转节点  $r_k$  发送的  $SEND_{r_0}$  后, 用私有密钥  $SK_s$  解密得到发送节点  $r_0$  的密钥  $K_0$ , 用密钥  $K_0$  再次解密, 得到举报信息  $P$ , 最后用密钥  $K_0$  对将要回复的内容进行加密。

举报受理机构向举报人回复确认信息的具体实现过程如下:

1) 举报受理机构收到举报信息  $P$  之后, 先给该举报信息  $P$  分配一个唯一的信息标识号  $ID_p$ , 同时利用 SHA-1 算法作用于举报信息  $P$ , 生成举报信息摘要  $MA$ , 其密钥为  $K_a$ , 即  $MA = K_a(P)$ 。再将信息摘要  $MA$ 、信息标识号  $ID_p$ 、 $K_a$  组合在一起, 并用举报受理机构的私有密钥  $SK_s$  对其进行加密得到确认信息  $MAI$ , 即  $MAI = E_{SK_s}(MA, ID_p, K_a)$ 。

2) 举报受理机构调用算法 3 将  $MAI$  返回给发送

节点。

3) 举报受理机构调用匿名通信协议中的服务器回复确认信息算法将确认信息返回给发送节点  $r_0$ 。

4) 发送节点  $r_0$  收到该信息后, 则用自己的私有密钥  $SK_{r_0}$  解密得到对称密钥  $K_{2i}$ , 再用  $K_{2i}$  解密信息, 得到密文, 最后用本身的密钥  $K_0$  对密文进行解密, 得到信息摘要  $MA$ 、举报信息标识号  $ID_p$ 、密钥  $K_a$ , 再用  $K_a$  解密得到举报信息  $P$ 。到此, 举报人确认自己的举报已被受理, 而且举报信息未被篡改。

$$\begin{aligned} & (D'((E(id, K_0(MAI))), D(PK_i(K_{2i}))) = \\ & (D'(E(id, K_0(MAI))), SK_{r_0}(PK_i(K_{2i}))) = \\ & (D'(E(id, K_0(MAI))), K_{2i}) = \\ & D'(id, K_0(MAI)) = \\ & (id, MA, ID_p, K_a) \\ & D'(MA) = D'(K_a(P)) = P \end{aligned}$$

同时, 举报人以  $K_a$  为密钥, 使用 SHA-1 算法作用于举报信息  $P$ , 生成摘要  $MA_1$ , 即  $MA_1 = K_a(P)$ 。如果  $MA_1 = MA$ , 则举报人确认举报信息未被篡改。

至此, 举报人利用匿名通信协议完成了匿名举报, 并得到了举报受理机构的回复。在整个过程中, 每个节点(包括举报受理机构)都只知道发送信息给自己的上一个节点, 无法知道发送举报信息的节点是谁。中转节点  $r_1$  虽然知道发送节点  $r_0$  的位置, 但是无法知道  $r_0$  就是举报人, 实现了对举报人身份和位置隐私的保护。

#### 算法5 举报受理机构发送回复消息算法

1. 举报受理机构收到消息  $SEND_{r_0}$  后, 用私有密钥  $SK_s$  给解密得到密钥  $K_0$ , 继续解密得到举报消息  $P$ ;
2. 举报受理机构给该举报消息分配一个唯一的信息标识号  $ID_p$ ;
3.  $MA = K_a(P)$ ; // 举报受理机构用 SHA-1 算法生成举报消息摘要  $MA$
4.  $MAI = SK_s(MA, ID_p, K_a)$ ; // 举报受理机构用其私有密钥  $SK_s$  加密  $MA, ID_p, K_a$ , 得到确认信息  $MAI$
5.  $m = K_0(MAI)$ ; // 用密钥  $K_0$  加密  $MAI$
6.  $c_1 = K_s(ID, m)$ ; // 举报受理机构用其对称密钥  $K_s$  加密  $ID$  号和  $m$
7.  $c_2 = PK_i(K_s)$ ; // 用  $ID$  号对应节点的公开密钥  $PK_i$  加密  $K_s$
8.  $ANS_{r_0} = (c_1, c_2)$  // 举报受理机构生成回复消息
9. 举报受理机构调用算法 3, 完成消息  $ANS_{r_0}$  的发送;
10. 中转节点  $r_1$  接收  $ANS_{r_0}$  后, 调用算法 2 进行转发操作;
11. 举报人收到  $ANS_{r_0}$  后, 用其私有密钥  $SK_{r_0}$  和对称密钥  $K_0$  进行解密, 获得回复信息  $P_1$ ;
12.  $MA_1 = K_a(P)$ ; // 举报人用 SHA-1 算法生成举报消息摘要  $MA_1$
13. if( $MA_1 == MA$ ) then 举报信息未被篡改。

### 1.3 举报人奖励

若举报信息被证实为真, 举报受理机构要给予举报人奖励。

1) 举报受理机构在自己网站上的公告板上公布  $PM =$

$\langle ID_p, E_{K_0}(s) \rangle$ , 其中,  $ID_p$  为举报信息标识号,  $E_{K_0}(s)$  为使用  $K_0$  对随机字符串  $s$  加密后的结果。

2) 真正的举报人可以根据自己的举报信息标识号  $ID_p$  检索公告板得到  $PM$ , 然后利用  $K_0$  解密  $E_{K_0}(s)$  即可得到  $s$ 。

3) 举报人得到  $s$  之后, 仍然使用匿名通信协议将信息“ $s$ +安全的收款方式”发送给举报受理机构。其中, 安全的收款方式可能是一个匿名转账账户, 收到汇款时自动转给举报人的账户, 也可能是一家金融代理机构的账户, 它再转给举报人账户。相关法律保证了匿名转账账户经营者或者金融代理机构必须保证客户隐私, 不得将汇款去向透露给包括举报受理机构在内的任何组织和个人。因此, 不可能通过追踪奖金去向而发现举报人身份。

4) 举报受理机构收到之后, 先进行解密, 验证  $s$  和  $ID_p$ , 以确认举报人真实性, 再将奖金根据该收款的要求汇出, 至此完成了对举报人的奖励。

#### 算法6 奖励举报人算法

1.  $E_{K_0}(s) = K_0(s)$ ; // 举报受理机构用密钥  $K_0$  加密随机字符串  $s$
2.  $PM = \langle ID_p, E_{K_0}(s) \rangle$ ; // 举报受理机构在自己网站公告板上公布  $PM$
3. 举报人根据举报信息标识号  $ID_p$  检索公告板得到  $PM$ ;
4.  $D'(E_{K_0}(s)) = s$ ; // 举报人用  $K_0$  解密  $E_{K_0}(s)$ , 得到随机字符串  $s$
5.  $c_1 = K_0(s, pay)$ ; // 用密钥  $K_0$  对加密随机字符串  $s$  和安全的付款方式  $pay$
6.  $c_2 = PK_s(K_0)$ ; // 用举报受理机构的公开密钥  $PK_s$  加密  $K_0$
7. 生成举报人要发送消息  $SEND_{r_0} = (c_1, c_2)$ ;
8. 举报人作为初始发送节点  $r_0$  调用算法 1, 将消息  $SEND_{r_0}$  发送给中转节点  $r_1$ ;
9. 中转节点  $r_1$  收到消息  $SEND_{r_0}$  后, 调用算法 2 进行消息的转发操作;
10. 举报受理机构将奖金根据该付款方式的要求汇出, 完成奖励。

## 2 方案性能分析

### 2.1 有效性分析

举报消息在传送过程中, 所有的相关节点都是对等的, 不存在需要依赖的某些特殊节点。因此, 如果网络中任意节点发生故障, 不会对举报消息的正常发送产生影响, 这是因为该方案具有完全自组织、无中心的特点。同时, 任何一个节点出现问题都不会对整个举报消息的发送过程产生影响, 即使存在恶意节点的合谋攻击, 也无法得到完整的通信线路, 除非攻击者与节点中除举报人节点和举报受理机构以外的所有节点一起合谋, 显然这是一个极小概率事件。举报消息要发送到举报受理机构, 举报受理机构的回复消息要返回给举报人, 那么成功建立一条通信路径至关重要。通信路径的可达和可靠是该方案有效的一个前提。



该方案以固定的转发概率完成重路由路径选择, 记转发概率为  $p_f$ , 路径长度为  $L=k+1$ ,  $k$  为转发次数(中转节点个数)。经过  $k$  次转发, 信息仍未发送到举报受理机构的概率为:

$$P_e = (p_f)^k \quad (1)$$

取  $p_f=1/2$ ,  $L=8$ , 则:

$$P_e = (1/2)^7 = 0.0078 \quad (2)$$

举报人发送的举报信息经过较少几次(不超过7次)转发之后, 仍然不能到达举报受理机构的概率仅为0.78%, 这个概率基本上可以忽略不计。

为保障举报信息百分之百到达举报受理机构获得受理, 可以约定举报者等待一段时间  $T_A$  之后仍未收到举报服务器的确认, 则重发举报信息,  $T_A C$  称为重发阈值。由于现实中对于举报者而言, 重要的是举报受理机构确定收到举报信息, 而获得举报服务器快速乃至实时回复并不是必要的, 因此,  $T_A$  可以选取相对较长的一段时间, 例如1 h, 这样可以避免举报者多次发送重复的信息。容易看到, 最多经过几次重发, 举报者收到举报受理机构的确认信息的概率接近于100%。

综上所述, 该方案可以有效地实现举报人将举报消息发送给举报受理机构, 具有很好的可行性。

## 2.2 平均路径长度

设转发概率为  $p_f$ , 一次消息发送过程的路径长度为  $L=k+1$ 。根据概率论, 路径长度恰好为  $L$  的概率如下:

$$P_L = (p_f)^{L-2} (1-p_f) \quad (3)$$

则平均路径长度如下:

$$\tilde{L} = \sum_{L=2}^{\infty} L P_L = \sum_{L=2}^{\infty} L (p_f)^{L-2} (1-p_f) = \frac{2-p_f}{1-p_f} \quad (4)$$

容易看到, 平均路径长度只和转发概率有关, 转发概率越大, 平均路径长度越长。

## 2.3 健壮性

在本文的匿名举报方案中, 所有的中转节点都是随机选出来的, 不依赖于网络中任何特定的节点, 因此不会因为任何节点的故障或者性能瓶颈导致举报消息无法顺利发送。理论上讲, 无论网络中有多少个节点出现故障, 只要还有少数  $n$  个节点 ( $n$  大于等于平均路径长度) 正常工作, 举报消息仍然可以正常发送。因此, 该方案具有很好的健壮性。

## 3 安全性分析

### 3.1 安全性证明

基于匿名通信技术的匿名举报方案主要涉及3种隐私的安全性保护, 分别是举报人身份隐私、举报人位置隐私和举报内容隐私。其中, 举报人身份和位置的隐私是指在举报的全过程中, 举报受理机构、任意中转节点和攻击者都不能获取举报人的身份和地理位置信息。举报内容的隐私是指在举报消息的转发过程中, 任意中转节点和攻击者都无法获得举报消息内容<sup>[18-20]</sup>。

**定理1** 举报人身份信息是保密的, 包括举报受理机构在内的任何人都无法获取。

**证明** 举报人将经过加密的举报消息进行发送, 在举报消息中不包含任何与自己身份有关的内容。举报受理机构只能获取举报消息而不能获取举报人的身份信息。任意的中转节点或者攻击者只能得到举报消息的密文, 因为没有举报机构的私有密钥, 所以无法解密密文, 也无法获取任何有用信息, 包括举报人的身份信息。

**定理2** 举报人位置是保密的, 包括举报受理机构在内的任何人都无法获取。

**证明** 举报受理机构收到举报信息后, 能够确定的只是把举报消息发给它的那个节点(即最后一个转发消息的节点), 根据匿名通信协议, 显然这个节点一定不是举报者。即使该节点与举报受理机构合谋, 它们仍然无法确定举报者, 因为该节点知道的也只是上一个转发消息给自己的节点, 根据匿名通信协议, 它可能是举报节点, 更可能只是倒数第2个中转节点。而且由于中转节点都是随机选择的, 因此举报受理机构想得到任意一条转发路径中的所有中转节点的支持来回溯举报者是一个概率极小的事件, 在现实中不可能发生。而且, 即使整个消息转发路径上的所有中转节点都参与合谋, 举报受理机构能够沿着转发路径回溯到第一个转发节点, 仍然无济于事。因为第一个转发节点只知道消息是上一个节点(事实上的举报者)发给自己的, 但是并不能确定该节点就是举报者。

如果一个中转节点想要获取举报者的位置信息, 它所知道的也只是上一个转发消息给自己的节点, 能做的事情也只是如上述举报受理机构一样地设法回溯(获取路径前方所有中转节点支持的前提下)。这不但是极其困难(实质上不可行), 而且即使回溯到第1个中转节点, 仍然无法确定发送者。

任意的外来攻击者只能监听信道上传输的数据, 而这些数据都是加密的, 它不可能得到任何有意义的信息。另一方面, 即使外来攻击者攻破了部分乃至全部中转节点, 也只是相当于部分(后者全部)节点与攻击者合谋, 根据上面的论证可以看出, 攻击者仍然无法获取举报者的位置信息。

**定理3** 举报消息内容是秘密的, 除了举报受理机构外, 任意中转节点和攻击者都不可能获得举报消息的内容。

**证明** 第  $i$  个中转节点接收到上一个节点发送的消息  $SEND_{r_0} = (c_1, c_2, c_3) = (K_i(s, K_0(P)), PK_s(K_0), PK_i(K_i))$  后, 经过解密, 只能得到序列号  $s$ 、加密的密文  $K_0(P)$  以及  $K_i$ , 其中, 经过加密的密文中包含举报人的举报信息  $P$ , 但是加密的密文  $K_0(P)$  需用密钥  $K_0$  才能解密, 而  $K_0$  是由举报受理机构的公有密钥加密, 由公开密钥算法可知,  $K_0$  只能由举报受理机构的

私有密钥才能解密。因此,中转节点不能获得举报人发送的举报消息的内容 $P$ 。

任意的攻击者只能截获在信道中传输的数据报,而根据匿名通信方案,举报消息是经过发送者的密钥 $K_0$ 和中转节点的密钥 $K_i$ 的双重加密的。攻击者不可能得到这两个密钥,因而没有办法恢复出举报消息原文。

可以证明举报受理机构发给举报者的确认消息也是秘密的。中转节点收到举报受理机构发送的回复确认消息 $ANS_{r_i}=(K_s(s, K_0(P_i)), PK_i(K_s))$ 后,通过解密该消息,中转节点可以获取该消息的序列号 $s$ 和密文 $K_0(P_i)$ 。由对称密钥算法可知,密文只能通发送节点的对称密钥 $K_0$ 才能解密,而 $K_0$ 只有举报人和举报受理机构才有。因此,中转节点不能获取举报机构的回复确认消息的内容。同理,攻击者也不可能获取。

### 3.2 匿名度

在匿名举报方案中,举报消息至少经过一个节点的转发才能到达举报受理机构,一般情况下是经过多个中转节点转发的。因此,举报受理机构可以断定发送举报消息给自己的节点一定不是举报者。如果举报受理机构想要获取举报者的身份,它可能与中转节点合谋,设法沿着转发路径回溯到举报节点。当然,对于忠实可靠的中转节点来说,它会拒绝与举报受理机构合谋,导致举报机构的企图失败。然而,举报受理机构有可能事先在网络中安排若干数量的恶意节点,如果这些节点被选为中转节点,它就可以借助这些恶意节点的同谋来追溯举报者。

假定网络中共有 $N$ 个可能的中转节点(除举报受理机构和举报者外),其中有 $K$ 个节点是恶意节点。如果一次举报过程中路径长度为 $L=2$ ,即只有一个中转节点,而这个节点恰巧是恶意节点,那么举报受理机构与该节点合谋,就可以确定举报者就是发送消息给该恶意节点的上一个节点,从而发现了举报者的身份。由于中转节点是随机选择的,因此一个恶意节点被选中的概率是 $K/N$ ,而根据式(3),路径长度为2的概率为 $(1-p_f)$ ,所以,举报代理机构获取举报者身份的概率为 $K(1-p_f)/N$ 。推对于任意的路径长度 $L \geq 2$ ,举报代理机构发现举报者身份的概率如下:

$$P(L, K, N, p_f) = \frac{K}{N} \times \cdots \times \frac{N-L+2}{N-L+2} \times P_L = \left( \prod_{i=0}^{L-2} \frac{K-i}{N-i} \right) \times (p_f)^{L-2} (1-p_f) \quad (5)$$

因此,在一般情况下,举报代理机构发现举报者身份的平均概率如下:

$$\tilde{P}(K, N, p_f) = \sum_{L=2}^{\infty} P(L, K, N, p_f) \quad (6)$$

定义匿名度如下:

$$D = 1 - \tilde{P}(K, N, p_f) \quad (7)$$

假定节点总数 $N=100$ ,图2给出了匿名度随恶意节点个数的变化曲线。可以看到,在一定的转发概率下,恶意节点数量越多,匿名度就越低,这是符合预期的,因为恶意节点越多,与举报代理机构同谋的节点就越多,后者获得举报者身份的概率就越大,相应地,匿名度越低。另一方面,当恶意节点数量确定时,转发概率越大,匿名度就越高,因为转发概率越大,举报消息在到达举报代理机构之前经过的转发次数就越多,转发路径越长,相应地,举报代理机构回溯到举报者的概率就越低。最后,当恶意节点数量为50时,即网络中恶意节点数量达到了全部节点数量的50%,这在现实中是不可能出现的,但3种转发概率下的匿名度都超过了0.5。而当恶意节点数量为10时(比例为10%),3种转发概率下的匿名度都超过了0.9,当转发概率为0.75时,匿名度达到了0.95。在现实中,举报代理机构面向全社会接受举报,网络中恶意节点的比例通常远小于10%,匿名度还会进一步提高。可见,本文方案能够有效地保证举报者的身份隐私。

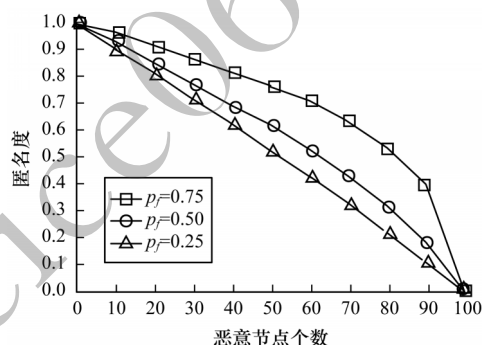


图2 匿名度与恶意节点个数的关系

Fig.2 Relationship between anonymity degree and number of malicious nodes

## 4 实验结果与分析

### 4.1 实验环境

实验的硬件环境:CPU为Intel® Pentium® CPU i5-8265U @ 1.80 GHz;内存为24.00 GB;操作系统为Windows 10。实验的软件环境:基于Eclipse Mars, x64平台, jdk-8.0.2。

### 4.2 结果分析

图3给出当转发概率 $p_f$ 分别等于0.25、0.50、0.75时,随着网络节点总数的不断增加举报消息的平均路径长度的变化。可以看出,平均路径长度在恒定值上下小范围波动,没有明显变化。这与3.2节关于平均路径长度的理论计算是一致的。从图3还可以看出,在节点数一定的情况下,转发概率不同,节点

的平均转发路径长度也不同。当转发概率为 0.25 时,平均路径长度较短,约为 2.3;当转发概率为 0.50 时,平均路径长度适中,约为 3;当转发概率为 0.75 时,平均路径长度同样较长,大概为 5。显然,平均路径长度越长,方案的匿名性越好,相应地,通信时间会延长,网络负载会更重。在现实中采用哪一个转发概率,要根据实际情况而定。

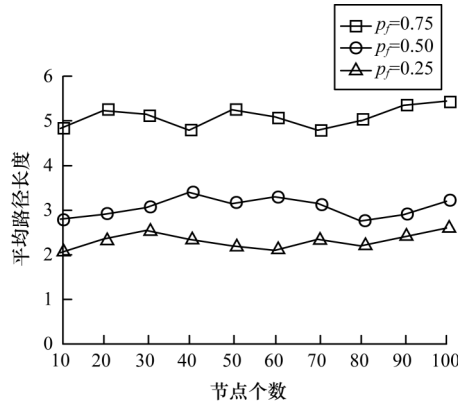


图3 节点数与平均路径长度的关系

Fig.3 Relationship between number of nodes and average path length

响应时间表示在正常通信过程中节点发送消息,举报代理机构处理一次消息所用的时间,即从举报者发送举报消息开始到发送者接收到举报代理机构的确认消息为止的总时间。平均响应时间为一段时间内所有举报者的响应时间的平均值。假定网络中共有  $n$  个节点,每一个节点都在同一时刻发送消息,假定  $x_i$  是节点发送消息的次数,  $t_{jx_i}$  是举报代理机构收到第  $j$  个节点发送的第  $x_i$  次消息并对其进行处理所用的时间,  $m$  是所有节点共同发送消息的次数。其中,  $m = x_1 + x_2 + \dots + x_n$ , 且  $m \neq 0$ 。平均响应时间如下:

$$T = \frac{\sum_{j=1}^n \sum_{i=0}^n t_{jx_i}}{\sum_{i=1}^n x_i} \quad (8)$$

图4表示当转发概率  $p_f$  分别等于 0.25、0.50、0.75 时,随着网络节点总数的不断增加平均响应时间的变化趋势。可以看出,当节点数目确定时,转发概率越大,平均响应时间越长。这是因为平均路径长度随着转发概率的增大而增大,导致举报消息经过更多次转发,平均响应时间自然随之增加。当转发概率确定时,随着节点数目增加,平均响应时间也随之增加。这是因为网络中有更多的举报者发送举报消息,每一个节点需要承担更多的转发任务,举报受理机构也需要接受更多的举报消息及回复,同时网络信道上的负载也更大,导致完成一次举报和确认过

程的时延相应增加。然而,无论在哪一种转发概率下,平均响应时间基本上是线性增长,并没有出现平均响应时间急剧增长导致系统反应缓慢乃至瘫痪的情况。因此,该方案是稳定和可靠的。

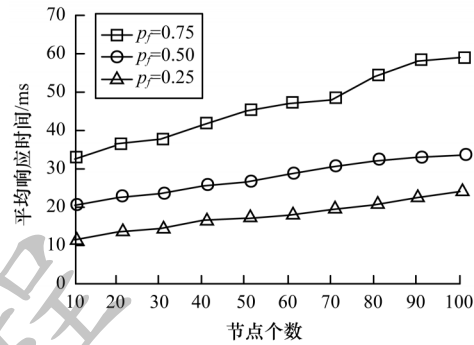


图4 节点数与平均响应时间的关系

Fig.4 Relationship between number of nodes and average response time

图5表示当转发概率分别为 0.25、0.50、0.75 时,每一个节点的平均转发流量。从图5可以看出,当转发概率确定时,随着节点数目的增加,节点的平均转发流量基本维持不变,只有小幅度的波动,其原因是网络节点数量增加,则举报者数量也增多,举报消息相应增加。但是,参与转发的节点数量也随之增加,通过平均,每一个节点转发的消息流量基本保持恒定。因此,本文方案可以均衡地分配网路流量,避免因为某些节点负载过大而造成的网络拥塞。另一方面,当网络节点数量确定时,随着转发概率的增大,节点的平均转发流量也增加,原因是转发概率增大,意味着每条举报消息被转发的次数也相应增加,网络中转发的总流量也相应增加,所以节点平均转发流量随之增加。

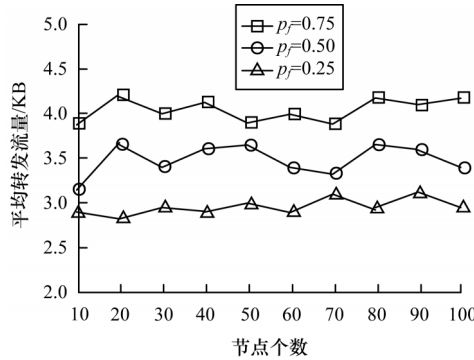


图5 节点数与平均转发流量的关系

Fig.5 Relationship between number of nodes and average forwarding traffic

表2是在软硬件配置环境一致的情况下本文方案与已有的其他方案的性能对比。可以看出,本文方案在转发概率取 0.50、0.75 时,平均响应时间均比已有的匿名举报方案更短,性能更优。



表2 不同方案的平均响应时间对比

Table 2 Comparison of average response time of different schemes ms

匿名举报方案	50个节点平均响应时间	100个节点平均响应时间
文献[9]方案	88.5	101.2
文献[12]方案	103.9	120.6
文献[17]方案	53.1	69.0
本文方案( $p_f=0.50$ )	26.2	34.1
本文方案( $p_f=0.75$ )	45.0	58.3

## 5 结束语

本文提出一个基于匿名通信的在线匿名秘密举报方案。匿名举报者使用匿名通信技术将举报信息发送给受理机构,举报受理机构、中转节点以及任意的攻击者都不可能获得举报者的身份信息和地理位置,除举报者和举报受理机构之外的任意第三方也无法获取举报信息。举报被证实后,举报人可以获得奖励,同时仍然保持身份隐私。该方案不依赖于网络中的特定节点,对网络流量的负载能够实现有效均衡,健壮性比较好。实验结果表明,随着通信过程中节点数目增多,系统的平均响应时间不会出现急剧增长以至于发生系统瘫痪的情况,具有良好的可靠性和稳定性。本文没有考虑中转节点可能掉线引起的举报确认信息无法返回给举报者情况,下一步拟采用多路由转发方案,以确保举报确认信息到达举报者。

## 参考文献

- [1] WU Y H, WANG W P, CHEN J E. An overview of anonymous communication research[J]. Small Microcomputer System, 2007, 28(4): 583-587.
- [2] CHAUM D L. Untraceable electronic mail, return addresses, and digital pseudonyms[J]. Communications of the ACM, 1981, 24(2): 84-89.
- [3] PIZZIO R, UCHÔA-FILHOB F, RENZO M D, et al. Generalized spatial modulation for downlink multiuser MIMO systems with multicast[C]//Proceedings of the 27th IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications. New York, USA: ACM Press, 2016: 1-6.
- [4] 胡德敏,詹涵. 差分扰动的均衡增量近邻查询位置隐私保护方法[J]. 小型微型计算机系统, 2018, 39(7): 1483-1485.
- [5] HU D M, ZHAN H. Homogeneous incremental nearest neighbor query method based on differential perturbation for location privacy protection[J]. Journal of Chinese Computer Systems, 2018, 39(7): 1483-1485. (in Chinese)
- [6] 何明星,李鹏程,李斌. 高效的可证明安全的无证书数字签名方案[J]. 电子科技大学学报, 2015, 44(6): 887-891.
- [7] HE M X, LI P C, LI X. Efficient and provably secure certificate-less signature from bilinear pairings[J]. Journal of University of Electronic Science and Technology of China, 2015, 44(6): 887-891. (in Chinese)
- [8] 熊金波,王敏荣,田有亮,等. 面向云数据的隐私度量研究进展[J]. 软件学报, 2018, 29(7): 5-8.
- [9] XIONG J B, WANG M S, TIAN Y L, et al. Research progress on privacy measurement for cloud data[J]. Journal of Software, 2018, 29(7): 5-8. (in Chinese)
- [10] 谢永,吴黎兵,张宇波,等. 面向车联网的多服务架构的匿名双向认证与密钥协商[J]. 计算机研究与发展, 2016, 53(10): 2228-2331.
- [11] XIE Y, WU L B, ZHANG Y B, et al. Anonymous mutual authentication and key agreement protocol in multi-server architecture for VANETS[J]. Journal of Computer Research and Development, 2016, 53(10): 2228-2331. (in Chinese)
- [12] 苗付友,王行甫,苗辉,等. 一种支持悬赏的匿名电子举报方案[J]. 电子学报, 2008, 36(2): 320-324.
- [13] MIAO F Y, WANG X F, MIAO H, et al. An anonymous e-prosecution scheme with reward support[J]. Acta Electronica Sinica, 2008, 36(2): 320-324. (in Chinese)
- [14] 王化群,于红,吕显强,等. 一种支持悬赏的匿名电子举报方案的安全性分析及设计[J]. 电子学报, 2009, 37(8): 1826-1829.
- [15] WANG H Q, YU H, LÜ X Q, et al. Cryptanalysis and design of an anonymous e-prosecution scheme with reward support[J]. Acta Electronica Sinica, 2009, 37(8): 1826-1829. (in Chinese)
- [16] 吴韬,夏斌,邱卫东. 基于比特承诺的可撤销匿名电子检举系统[J]. 信息安全与通信保密, 2010, 48(1): 113-115.
- [17] WU T, XIA B, QIU W D. An impeaching system based on bit commitment with revocable anonymity[J]. Information Security and Communications Privacy, 2010, 48(1): 113-115. (in Chinese)
- [18] 张瑞丽,李顺东. 一种新的基于身份的匿名电子举报方案[J]. 计算机应用与软件, 2015, 32(1): 288-290, 294.
- [19] ZHANG R L, LI S D. A new identity-based anonymous electronic prosecution scheme[J]. Computer Application and Software, 2015, 32(1): 288-290, 294. (in Chinese)
- [20] NAYIR D Z, HERZIG C. Value orientations as determinants of preference for external and anonymous whistleblowing[J]. Journal of Business Ethics, 2012, 107(2): 197-213.
- [21] HUNTON J E, ROSE J M. Effects of anonymous whistleblowing and perceived reputation threats on investigations of whistle-blowing allegations by audit committee members[J]. Journal of Management Studies, 2011, 48(1): 75-98.
- [22] ESHGHI S, TASSIULAS L. Whistleblowing games in networks[C]//Proceedings of the 52nd Annual Conference on Information Sciences and Systems. New Haven, USA: IEEE Press, 2018: 1-6.
- [23] JAYAKRISHNAN H, MURALI R. A simple and robust end-to-end encryption architecture for anonymous and secure whistleblowing[C]//Proceedings of the 12th International Conference on Contemporary Computing. Piscataway, USA: IEEE Press, 2019: 6-15.
- [24] YOUNG J A, COURTNEY J F, BENNETT R J. The impact of anonymous, two-way, computer-mediated communication on perceived whistleblower credibility[J]. Information Technology & People, 2020, 35(6): 72-83.
- [25] 杨小东,陈桂兰,李婷,等. 基于无证书密码体制的多用户密文检索方案[J]. 计算机工程, 2020, 46(9): 129-135.
- [26] YANG X D, CHEN G L, LI T, et al. Multi-user ciphertext retrieval scheme based on certificateless cryptosystem[J]. Computer Engineering, 2020, 46(9): 129-135. (in Chinese)
- [27] BAKIRAS S, TROJA E, XU X H, et al. Secure and anonymous communications over delay tolerant networks[J]. IEEE Access, 2020, 8: 88158-88169.
- [28] NASCIMENTO B L C D, OLIVEIRA A R. Enabling anonymous whistleblowing through online reporting mechanisms in Brazil[C]//Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance. New York, USA: ACM Press, 2020: 783-786.
- [29] DATTA A, TIU A. On unlinkability and denial of service attacks resilience of whistleblower platforms[J]. Future Generation Computer Systems, 2021, 118: 438-452.