# 基于匿名路由的移动位置隐私保护

熊婉竹 李晓宇

(郑州大学信息工程学院 郑州 450000)

**摘 要** 为了保证移动节点在使用基于位置的服务时的位置隐私,提出基于匿名路由的移动位置隐私保护方法。该方法将移动网络中的每一个移动节点都当作可以使用的中转节点,采用重路由的方式进行路由选择,第一跳用随机选取的方式选择中转节点,剩下的路径选择通过一定的转发概率来确定下一跳并将其发送给中转节点或 LBS 服务器。为保证位置信息不被泄露,移动发送节点用目标服务器的公钥对地理位置信息和查询信息进行加密,再利用下一跳的公钥对已加密的内容进行二次加密,并转发给下一跳。同时中转节点收到后,用当前节点的私钥解密,解密时只能解密最外层,再用随机选取的下一跳的公钥加密,重复此过程,直至 LBS 服务器接收到移动发送节点发来的信息。理论分析和实验结果表明,这种移动位置隐私保护方式可以保证 LBS 服务器和任何中转节点都不能获取移动发送节点的位置隐私,可以在较低的代价下实现移动发送节点的位置隐私保护。并且在该方案中中转节点可以是移动网络中的任意一个节点,不会因为部分节点故障导致通信失败,因此所提方案的健壮性较好。

**关键词** 移动位置隐私,匿名路由,加密机制,安全性,匿名性

**中图法分类号** TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.10.027

## Mobile Location Privacy Protection Based on Anonymous Routing

XIONG Wan-zhu LI Xiao-yu

(School of Information Engineering, Zhengzhou University, Zhengzhou 450000, China)

**Abstract** To preserve the security of mobile location pravicy based on location services, a mobile location pravicy protection model based on anonymous routing was presented. This model makes every mobile node as a forwarder and uses rerouting to select a route. It uses random selected mobile node as first forwarder, queries issued by it are firstly encrypts with public key of the location information server and secondly encrypted with the public key of first forwarder. Then mobile sending node sends it to first forwarder. The first forwarder receives it and decides next hop which is either location information server or second forwarder, the first forwarder firstly decrypts it with private key of first forwarder, then secondly encrypts it with the public key of next hop. If next hop is second forwarder, it does what the first forwarder does until the location information server receives this message. Theoretical analysis and experimental results show that the mobile location privacy protection model can ensure the location privacy of location information server and any forwarder node can acquire mobile nodes, and it can realize the location privacy protection of a mobile node at a low price. Moreover, forwarder node can be any node in the mobile network, so this model is robust and can't fail due to the faults of some nodes.

**Keywords** Mobile location privacy, Anonymous routing, Encryption mechanism, Safety, Anonymity

## 1 引言

随着社会的发展,移动网络在人们生活中的使用频率越来越高,网络的安全性成为当今社会越来越重视的问题,其中用户位置隐私的保护成为了网络安全保护的重中之重。因为移动设备大都有 GPS 卫星定位功能,在使用基于位置的信息服务(Location Based Service, LBS)时,用户本身的位置以及运动轨迹就暴露了,这在很大程度上造成了用户个人信息的泄露[1]。这里所提到的基于位置的服务(LBS)就是通过 GPS 定位系统获取移动终端的位置信息,然后将位置信息发送给地理位置信息服务器,进而提供给移动终端基于地理位置的相关信息及服务。

匿名通信指采取一定的方法来隐蔽通信流中的通信关系,使窃听者难以获取或推知通信双方的关系及内容。文献[2]提出了 MIX 技术,该技术通过使用中间节点混杂来自多个用户的信息,使窃听者无法跟踪消息的传输路径,用于解决电子邮件的匿名问题。文献[3]提出了洋葱路由算法,Dingledine 等[4]提出了第二代的洋葱路由模型 TOR,其基于洋葱

到稿日期:2017-09-11 返修日期:2017-12-08 本文受国家自然科学基金资助项目(61472412),河南省教育厅自然科学基金(14A520012)资助。

**熊婉竹**(1993—),女,硕士生,主要研究方向为移动安全、移动计算、位置隐私保护;**李晓宇**(1974—),男,博士,副教授,主要研究方向为量子计算与量子信息、移动计算、移动安全,E-mail:iexyli@zzu.edu.cn(通信作者)。

路由模型实现节点之间的匿名交流，用于抵御流量分析攻击。Reiter 等[5]提出了 crowds 匿名通信系统，采用重路由的机制进行匿名保护，主要提供匿名 Web 访问。

为了解决移动位置服务中的隐私保护问题[6]，文献[7]提出了 K-匿名模型，将 $k-1$ 个不同的元素与真实用户位置相融合并发给 LBS 服务器，实现位置的匿名。罗建等[8]提出了一种将假名匿名和位置匿名相结合的方法，采用了中心服务器模型，这种模型能实现较好的匿名效果，但当用户匿名等级提高时，结果利用率会变低，响应时间会增加。文献[9]详细介绍并总结了最新的位置隐私保护模型，并对不同方案下的 K 匿名方案进行了总结。文献[10]基于空间混淆的位置隐私保护方法，提出了两种隐私切换时的位置隐私区域的生成算法，当服务要求质量较高时，位置的模糊程度受到限制，使得位置信息不能得到足够保护。除 K-匿名方案、基于位置混淆的方案外，还有基于转换的方案[11]，其通过加密技术将所有数据转化到一个不同的空间，使其对 LBS 服务器完全不可见。

为了解决安全性问题，本文将匿名通信与位置隐私相结合，设计了一种基于匿名路由的移动位置隐私保护方案。这种匿名路由模式继承了 Crowds 方案中随机发送的思想，同时做了重大改进。本文在整个通信过程中采用匿名路由机制，对查询信息进行 AES 和 RSA 混合加密，地理位置信息服务器无法获取移动终端的位置隐私，也无法获知发送节点所在的大致区域，最终达到保护移动终端位置隐私的目的。针对文献[10-11]提出的移动位置隐私保护中健壮性的问题，本文方案在路径上不依赖某些特殊节点，网络中任意部分节点的故障不影响基于位置的服务的正常实现。同时，该方案实现了网络流量的平均分配，不会因为局部节点负载过重而导致网络阻塞。本文第 2 节介绍提出的匿名路由模型；第 3 节介绍模型安全性证明；第 4 节给出实验；最后总结全文并展望未来。

## 2　匿名路由模型

该模型的基本思路是当移动终端向 LBS 服务器发出基于位置的查询时，采用匿名路由机制使 LBS 服务器无法知道查询请求来自哪一个移动终端，从而保护移动终端的位置隐私。匿名路由机制是将同一个移动网络中的用户都视为等同的节点，当发送节点查询到与当前位置相关的信息时，查询信息不会直接发送给 LBS 服务器，而是经过随机选择的中间节点进行转发，采用对称加密和非对称加密相结合的方式实现对信息的加密保护。每个网络中的节点都可能成为信息转发路径中的一个节点，转发路径上的每个节点都会对加密信息的最外层进行加解密处理，使得该信息只与当前节点和下一随机选择的节点有关。返回过程沿原路径返回。这个机制可以保证发送节点的匿名性，使任意中间节点和目标服务器都不知道该信息的发送节点。在整个通信过程中，所有的信息都是加密的，路径中的转发节点不能获取到任何信息。对于 LBS 服务器来说，它会获得发来的位置信息，但是不知道是哪一个终端的位置信息。这是通过上述的匿名机制实现的。

### 2.1　匿名路由模型

所有的节点（包含服务器）都是公开密钥系统的成员。每个节点都有一对密钥：一个公钥 $PK_{id}$（Public Key for $\text{User}_{id}$）和一个私钥 $SK_{id}$（Secret Key for $\text{User}_{id}$）。简易的匿名查询模型如图 1 所示。

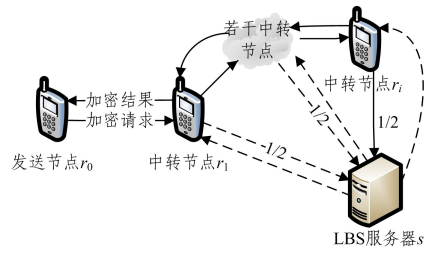


图 1　匿名路由模型

Fig. 1　Anonymous router model

详细的查询过程如下：

1）移动主机 $r_0$（即发送查询请求的节点）打算向服务器查询与自身地理位置相关的服务信息。发送的请求信息包含 3 部分内容。第一部分内容将采用发送节点的对称密钥 $K_0$ 对当前地理位置信息进行加密，然后将序列码（其中序列码是随机生成的并且不会重复）和这部分加密内容进行组合，用移动主机的对称密钥 $K_1$ 对其进行加密；第二部分内容用目标服务器 $s$ 的公开密钥 $PK_s$ 对发送节点的对称密钥 $K_0$ 进行加密；第三部分内容用随机选择的中转节点 $r_1$ 的公开密钥 $PK_1$ 对发送节点的对称密钥 $K_1$ 进行加密。该信息不直接发给 LBS 服务器，而是发给中转节点 $r_1$。

2）中转节点 $r_1$ 收到信息后，用 $r_1$ 的私有密钥 $SK_1$ 解密，得到发送节点的对称密钥 $K_1$，利用解密得到的 $K_1$ 解密信息的第一部分，从而得到序列号，记录下序列号和发送的源 IP 地址，并存入简易路由表 $t_1$ 中，如表 1 所列（每个节点 $i$ 中都存有一个对应的表格 $t_i$）。然后以 50% 的概率发给目标服务器，以 50% 的概率发给除了 $r_1$ 和 $r_0$ 之外的节点中随机选出的中转节点 $r_2$。不论发给谁，都是先用当前节点的对称密钥 $K_2$ 对序列码和密文加密，第二部分的内容保持不变，再用选出的下一个节点的公开密钥 $PK_2$ 对当前节点的对称密钥 $K_2$ 进行加密，同样是将三部分内容组成的信息加密转发（选择 1/2 的转发概率是为了保证转发次数不会太小）。

表 1　简易路由表 $t_i$

Table 1　Simple routing table $t_i$

| seq | Last Previous_IP |
|---|---|
| … | … |

3）中转节点 $r_2$ 进行步骤 2）中同样的操作，记录下序列号和信息源 IP 地址（即上一个中转节点 $r_1$ 的 IP 地址），并存入表 $t_2$ 中。以同样的概率发送给目标服务器或者是中转节点 $r_3$，经过 8 个中间节点的转发仍未发送到服务器的概率很小，可以忽略不计。

4）服务器 $s$ 在收到中转节点 $r_i$ 转发的信息后，用自己的私有密钥 $SK_s$ 解密，得到上一个中转节点的对称密钥 $K_{2i}$ 和发送方的第一个对称密钥 $K_0$，利用这两项来对信息的第一部分进行解密，得到序列号和发送节点发来的地理位置信息 $P$，同样地，将该信息的序列号和上一个中转节点的 IP 地址存入到表 $t_s$ 中。

至此，服务器收到一个包含节点地理位置信息的查询请

求，但是不知道是哪一个节点发来的。

服务器回复初始发送节点信息的过程如下：

1)服务器向发送节点回复的信息为 $P_1$，回复的信息包含两部分。第一部分是使用解密得到的原始发送节点的密钥 $K_0$ 对 $P_1$ 进行加密，得到密文后将序列码和密文组成信息，再用服务器的对称密钥 $K_s$ 对信息进行加密；第二部分是使用信息序列码对应节点的公开密钥 $PK_i$ 对服务器的对称密钥 $K_s$ 进行加密。最后根据查表得到该序列码对应的节点 IP 地址，将其发送给相应的中转节点 $r_i$(回复信息的序列码与原请求信息的序列码相同)。

2)中转节点 $r_i$ 收到服务器发来的信息后，用私有密钥 $SK_i$ 解密得到服务器的对称密钥 $K_s$，再用解密得到的 $K_s$ 对信息的第一部分进行解密，得到序列码和密文。用中转节点的对称密钥 $K_{2i}$对序列码和密文加密。然后查表 $t_i$，选择历史最新记录的同一个信息序列码所对应的节点的公开密钥 $PK_{i-1}$对对称密钥 $K_{2i}$加密。将表中查得的 IP 地址发送到节点 $r_{i-1}$，同时删除表中的该项记录。

3)如果中转节点 $r_{i-1}$收到该信息，则重复回复信息中的步骤 2)，转发回复信息；如果发送节点 $r_0$ 收到该信息，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，得到序列码和密文。最后用发送节点本身的密钥 $K_0$ 对密文进行解密，得到服务器发来的消息 $P_1$。

至此，完成了一次节点发送查询请求，服务器发送回复的过程。在整个过程中，每个节点(包括服务器)都无法知道发送请求的节点的身份，只知道上一个节点。中转节点 $r_1$ 即使知道发送请求节点 $r_0$ 的位置，也无法知道 $r_0$ 就是发送请求方。因此，这在很大程度上实现了对移动位置隐私的保护。

### 2.2 定义

$P$ 表示发送节点向服务器发送的明文查询信息。$K_0$ 和 $K_1$ 表示 AES 算法为发送节点生成的密钥。其中，$r$ 表示公开密钥系统的中转节点，$PK_s$ 表示服务器的公开密钥，$c$ 表示密文。

**定义 1** 移动发送节点 $r_0$ 的地理位置信息：$L_{r_0}=(X_{r_0},Y_{r_0})$。

**定义 2** 使用密钥 $K_0$ 对明文信息 $P$(包含地理位置信息 $L_{r_0}$和查询内容 $M_{r_0}$)进行加密，得到密文 $c$，$c=K_0(L_{r_0},M_{r_0})=K_0(P)$。

**定义 3** 位置隐私请求 $REQ_{r_0}$：用三元组($m_1$，$m_2$，$m_3$)($m_j$ 表示请求的第 $j$ 部分($j=1,2,3$))表示发送请求节点 $r_0$ 的请求信息 $REQ_{r_0}$，具体含义如下。

1)请求信息第一部分 $m_1$。初始节点使用密钥 $K_1$ 对序列码、密文加密得到 $m_1$($seq$ 表示消息的序列码)，$m_1=K_1(seq,c)=K_1(seq,K_0(P))$。

2)请求信息第二部分 $m_2$。使用目标服务器的公开密钥 $PK_s$ 对初始节点的对称密钥 $K_0$ 进行加密，得到 $m_2$，$m_2=PK_s(K_0)$。

3)请求信息第三部分 $m_3$。使用下一个节点的公开密钥 $PK_i$ 对初始节点的密钥 $K_1$ 进行加密，得到 $m_3$，$m_3=PK_i(K_1)$。其中，当 $i=1$ 时，$PK_i$ 只能是中转节点的公开密钥；当 $i>1$ 时，$PK_i$ 表示下一个中转节点。$r_i=s$ 时，$r_i$ 节点即为服务器 $s$，则 $PK_i=PK_s$，$SK_i=SK_s$。

$D'$表示用 AES 算法解密，$D$ 表示用公钥密钥算法 RSA 解密。

**定义 4** 移动节点(中转节点 $i$ 或者服务器 $s$)使用私有密钥 $SK_i$($SK_s$)对信息的第三部分 $m_3$ 进行解密(若为服务器，则将下式中的 $SK_i$ 全部替换成 $SK_s$)：

$$D(M_3)=D(PK_i(K_1))=SK_i(PK_i(K_1))=K_1$$

**定义 5** 使用定义 4 解密的结果对信息的第一部分 $m_1$ 进行解密：

$$D'(M_1)=D'(K_1(seq,K_0(P)))=(seq,c)$$

**定义 6** 服务器用私有密钥 $SK_s$ 对信息的第二部分 $m_2$ 进行解密：

$$D(M_2)=D(PK_s(K_0))=SK_s(PK_s(K_0))=K_0$$

**定义 7** 服务器使用定义 6 解密的结果将定义 5 解密过的结果二次解密，从而获得明文信息 $P$：

$$D'(seq,c)=D'(seq,K_0(P))=(seq,P)$$

设 $P_1$ 表示服务器向节点返回的回复信息，$c'$表示服务器加密的密文。

**定义 8** 服务器使用初始发送的对称密钥 $K_0$ 对回复信息 $P_1$ 进行加密，得到密文 $c'$，$c'=K_0(P_1)$。

**定义 9**(回复信息 $ANS_{r_0}$) 用两元组($m_1$，$m_2$)表示服务器对请求方提供的相应的查询回复服务 $ANS_{r_0}$。具体含义如下：

1)回复信息的第一部分 $m_1$。服务器使用对称密钥 $K_s$ 对密文 $c'$进行加密，得到 $m_1$，$m_1=E(seq,c')=E(seq,K_0(P_1))=K_s(seq,K_0(P_1))$。

2)回复信息的第二部分 $m_2$。服务器使用收到的上一个同一序列码的节点的公有密钥 $PK_i$ 对对称密钥 $K_s$ 进行加密，得到 $m_2$，$m_2=E(K_s)=PK_i(K_s)$。

当 $r_0=i$ 时，当前节点即为初始发送节点，$SK_i=SK_{r_0}$。

**定义 10** 初始发送节点使用 $K_{2i}$和私有密钥 $SK_{r_0}$ 以及自身的对称密钥 $K_0$ 对回复信息进行解密，得到明文的回复信息 $P_1$：

$$\begin{aligned}&(D'((E(seq,c')),D(PK_i(K_{2i})))\\&=(D'(E(seq,c')),SK_{r_0}(PK_i(K_{2i})))\\&=(D'(E(seq,c')),K_{2i})\\&=D'(seq,K_0(P_1))\\&=(seq,P_1)\end{aligned}$$

### 2.3 基于位置的服务过程

移动节点使用基于位置的服务时，将当前位置信息及相关的查询请求打包，通过匿名路由模型经若干中转节点将与位置相关的查询请求发送给 LBS 服务器。

整个通信系统中，每个移动节点均用 RSA 算法生成一对密钥：公有密钥 $PK_i$ 和私有密钥 $SK_i$。需向服务器发送查询请求的移动节点用 AES 算法生成两个密钥 $K_0$ 和 $K_1$，$K_0$ 用于对发送节点的地理位置信息加密，$K_1$ 用于对序列号和已加密的部分组合起来加密。用服务器的公有密钥 $PK_s$ 对密钥 $K_0$ 进行加密；再用随机选择的中转节点的公有密钥 $PK_i$ 对密钥 $K_1$ 进行加密；将 3 部分内容组合起来得到真正要发送的信息。

**算法 1**　移动节点查询请求生成算法

1. 公开密钥系统为系统中的每个节点均分配一对公有密钥 $PK_i$ 和私有密钥 $SK_i$；
2. AES 算法为移动节点生成两个密钥，即 $K_0$ 和 $K_1$；
3. 移动节点 $r_0$ 向服务器申请服务器 s 的公有密钥 $P_{K_s}$；
4. $c=K_0(P)$；//用对称密钥 $K_0$ 加密 P
5. $m_1=K_1(seq,K_0(P))$；//$K_1$ 加密 seq 和密文 c
6. $m_2=PK_s(K_0)$；//$PK_s$ 加密 $K_0$
7. 用随机产生的中转节点的 $PK_i$ 加密 $K_1$，得 $m_3=PK_i(K_1)$；
8. 发送 $REQ_{r_0}=(m_1,m_2,m_3)$。

中转节点 $r_i$ 在收到移动主机发来的 $REQ_{r_0}$ 后，使用私有密钥 $SK_i$ 对 $m_3$ 进行解密，再对 $m_1$ 解密，获得序列号后，查询该信息的 *seq* 和发送该信息的 IP 地址是否存在于本地用户表 $t_i$ 中。若不存在，则将得到的序列号和移动主机 IP 地址存入表 $t_i$ 中，然后以 1/2 的概率随机选择下一个节点，不能返回给上一个发送方。使用当前节点的对称密钥 $K_{2i}$ 对序列号和密文进行加密，作为新的 $m_1$；$m_2$ 保持不变；用下一个节点的公有密钥 $PK_{i+1}$ 对当前节点的对称密钥 $K_{2i}$ 进行加密，作为 $m_3$。将信息发给下一节点 $r_{i+1}$；若 *seq* 和 IP 这两项内容都存在于表中，则利用对应 *seq* 的节点的公有密钥 $PK_{i-1}$ 对当前节点的对称密钥 $K_{2i}$ 进行加密，用 $K_{2i}$ 加密序列号和密文；最后将加密的信息转发给节点 $r_{i-1}$。整个转发路径长度控制在 10 以内，以保证通信时延不会太大。

**算法 2**　中转节点转发算法

```
1. for(i=0;i≤10;i++){
2.    中转节点 r_i 收到查询请求；
3.    D(m)=D(m_1,m_2,m_3)；//用私有密钥 SK_i 解密请求信息
4.    用对称密钥 K_1 解密信息，得序列号 seq 和密文 c；
5.    if(seq 和对应的发送方 IP 存在于表 t_i 中)then
6.       当前节点对密文加密；
7.       查询表 t_i，选择最新一条匹配的表项纪录，用 seq 所对应的节
         点的公有密钥 PK_{i-1} 对当前节点的对称密钥 K_{2i} 进行加密；
8.       发送给 seq 对应的 IP 地址的移动节点；
9.       删除最新的这条表项信息；
10.      break;
11.   else
12.      将 seq 和上一个节点的 IP 地址记录到表 t_i 中；
13.      if(rand()%2==0)then
14.         发送给目标服务器；
15.         当前节点 r_i 用其对称密钥和服务器 s 的公钥加密信息；
16.         break;
17.      else{
18.         在中转节点表中删除当前节点和上一个中转节点；
19.         随机选出一个中转节点，用选出的中转节点的公钥和当前节
            点的对称密钥加密信息；
20.         将信息转发给选出的中转节点 r_{i+1}；
21.         }
22.   }
```

服务器收到中转节点 $r_i$ 发送的 $REQ_{r_0}$ 后，用私有密钥 $SK_s$（$SK_s=SK_i$）解密得到对称密钥 $K_{2i}$ 和发送节点密钥 $K_0$，用 $K_{2i}$ 二次解密，得到序列号和密文，将序列号和上一个发送者的 IP 地址存入表 $t_s$ 中，再用密钥 $K_0$ 对密文 $c$ 进行解密，得到明文信息 $P$，最后用密钥 $K_0$ 对回复的内容 $P_1$ 进行加密。

**算法 3**　服务器解密并回复信息算法

1. $REQ_{r_0}=(m_1,m_2,m_3)=(K_{2i}(seq,K_0(P)),PK_s(K_0),PK_s(K_{2i}))$；//LBS 服务器收到查询请求
2. $D(m)=(K_{2i}(seq,K_0(P)),K_0,K_{2i})$；//私钥 $SK_s$ 解密 m
3. 用 $K_{2i}$ 对信息 m 进行解密，得到序列号 seq 和密文 c；
4. 将 seq 和上一个节点的 IP 地址记录到表 $t_i$ 中；
5. $D'(c)=P$；//$K_0$ 解密密文 c
6. 用密钥 $K_0$ 对回复信息 $P_1$ 进行加密，$c'=K_0(P_1)$；
7. $ANS_{r_0}=(K_s(seq,K_0(P_1)),PK_i(K_s)$//LBS 回复报文

整个通信过程包含节点发送请求、中转节点转发请求、LBS 服务器接收请求、节点接收回复 4 个阶段。具体实现如算法 4 所示。

**算法 4**　查询算法

1. 移动节点 $r_0$ 调用算法 1，将 $REQ_{r_0}$ 发给中转节点 $r_1$；
2. 中转节点 $r_1$ 接受 $REQ_{r_0}$，调用算法 2 进行中转节点转发操作；
3. 服务器收到 $REQ_{r_0}$ 后，调用算法 3，服务器发送 $ANS_{r_0}$；
4. 中转节点 $r_i$ 接收 $ANS_{r_0}$ 后，调用算法 2 进行转发操作；
5. 移动节点 $r_0$ 收到 $ANS_{r_0}$ 后，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 $P_1$。

最后，移动节点 $r_0$ 获取到 LBS 服务器返回的信息，完成了一次基于位置的服务。同时，在整个服务过程中，该方案保证了移动节点 $r_0$ 的地理位置不会被 LBS 服务器以及移动网络中的其他节点获取，从而实现了对移动节点的位置隐私保护。

## 3　性能分析

### 3.1　模型安全性分析

基于位置的服务查询[13]过程中涉及两种隐私：位置隐私和内容隐私。位置隐私是指地理位置服务器无法获知发送地理位置查询信息的节点身份。地理位置信息服务器实现了位置隐私。内容隐私是指路径上的中转节点不能推断出查询内容、发送节点的当前位置和查询结果。中转节点实现了内容隐私。

**定义 11**（位置隐私）　节点不能推断出发送节点的身份信息 *UID*。

**定义 12**（内容隐私）　节点不能推断出发送节点的查询内容 $M_{r_0}$、当前位置 $L_{r_0}$ 以及查询结果 $P_1$。

**定理 1**　中转节点实现了位置隐私。

证明：1）移动节点发送给中转节点的信息是 $REQ_{r_0}=(K_1(seq,K_0(L_{r_0},M_{r_0}),M),PK_s(K_0),PK_i(K_1))$。加密信息中没有与发送节点 *UID* 直接关联的内容，而且转发路径是随机确定的，因此中转节点不能获得发送节点的身份信息。

2）中转节点收到回复信息 $ANS_{r_0}=(K_s(seq,K_0(P_1)),PK_i(K_s))$。同样地，中转节点可以解密的信息中没有与发送节点的 *UID* 直接联系的内容，中转节点无法根据 $ANS_{r_0}$ 推断出发送节点的 *UID*。

**定理 2**　中转节点实现了内容隐私。

证明：1）中转节点收到的查询信息是 $REQ_{r_0}=(K_1(seq,K_0(L_{r_0},M_{r_0}),M),PK_s(K_0),PK_i(K_1))$。经过解密，只能得到序列号 *seq*、加密的密文 $K_0(L_{r_0},M_{r_0})$ 以及 $K_1$，加密的密文中包含发送节点的当前位置 $L_{r_0}$ 和查询内容 $M_{r_0}$。但是加密的密文 $K_0(L_{r_0},M_{r_0})$ 需要 $K_0$ 才能解密，而 $K_0$ 由 LBS 服务器的公有密钥加密，根据公开密钥算法，其只能由 LBS 服务器

的私有密钥才能解密。因此中转节点不能推断出发送节点的查询内容 $M_{r_0}$、发送节点的当前位置 $L_{r_0}$。

2)中转节点收到回复信息 $ANS_{r_0}=(K_s(seq,K_0(P_1)),PK_i(K_s))$。对信息解密得到序列号 $seq$ 和密文 $K_0(P_1)$,根据对称密钥算法,只有发送节点的对称密钥 $K_0$ 才能解密密文,因此中转节点不能推断出发送节点的查询结果。

**定理 3** LBS 服务器实现了位置隐私。

证明:LBS 服务器收到的查询信息是 $REQ_{r_0}=(K_i(seq,K_0(L_{r_0},M_{r_0}),M),PK_s(K_0),PK_i(K_i))$,通过层层解密,可以得到节点的当前位置 $L_{r0}$,但是由于匿名路由模型规定在发送节点与 LBS 服务器之间至少存在一个中转节点,因此 LBS 服务器无法推断出发送节点的身份信息 $UID$。

综上,LBS 服务器不能得到任何一条有意义的节点移动轨迹,从而保证了发送节点的位置隐私。

### 3.2 模型匿名性分析

本文所提出的匿名模型包括发送节点、中转节点和 LBS 服务器。发送节点的请求经过若干次转发后发送给 LBS 服务器,可以达到发送节点的匿名。如果攻击者想要知道发送节点,就必须控制发送节点之后的第一跳中转节点,同时至少要控制路径上过半的中间转发节点。

图 2 给出了一条被攻击者控制的匿名通信路径。有阴影的是恶意节点,不含阴影的为正常节点。恶意节点间隔地分布在整个通信路径上,而且发送节点的下一跳中转节点也是恶意节点,那么通过合谋攻击,攻击者就可以知道整条通信轨迹,最终知道谁是发送节点。

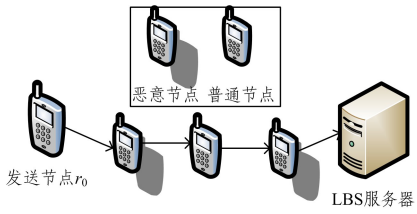


图 2 包含恶意节点的匿名路由模型

Fig. 2 Anonymous routing model containing malicious nodes

对于路径长度固定为 $L$ 的匿名通信路径,攻击者可以知道发送节点 $r_0$ 的概率:

$$p(r_0)=\begin{cases}C^{L/2+1}, & L \bmod 2=0\\ C^{(L+1)/2}, & L \bmod 2=1\end{cases}$$

其中,$C$ 为恶意节点占总节点数的比例。

本文提出的方案所建立的通信路径的长度是不固定的,而且每次的路径也不一定相同。因此,对每一条可能路径上发送节点被发现的概率求和,整个匿名路由发送节点被发现的概率为:

$$p(r_0)=\sum_{l=2}^{n}f^{l-2}(1-f)C^{\lceil(l+1)/2\rceil}=(1-f)\frac{fC^2+C}{1-f^2C}$$

其中,$f$ 为转发概率。

文献[17]将匿名性分为 6 个等级,之后采用概率 $p(x)$表示攻击者识别发送者和接收者的概率,$1-p(x)$表示系统的匿名度,即 $D=1-p(x)$。

图 3 对比了不同恶意节点占比下转发概率 $f$ 与匿名度之间的函数关系。从图 3 可以看出,随着转发概率的增大,匿名度也增大。同时,恶意节点比例越小,匿名度越大。

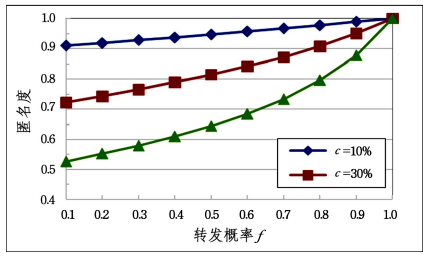


图 3 转发概率 $f$ 与匿名度的函数关系

Fig. 3 Function relationship of forwarding probability $f$ and anonymity

设发送节点向 LBS 服务器发送的服务查询数量是连续的,且每个发送节点在单位时间内发送的查询请求是独立、平稳的随机泊松过程。则概率函数 $p=P(X=i)$。其中 $i$ 表示 $X$ 可以取到每一个节点。文献[18]使用信息熵量化匿名度并衡量匿名通信的性能,提出了基于信息论模型的匿名度的定义:

$$D=\frac{E(x)}{E_{\max}}=\frac{-\sum p(x)\log(p(x))}{\log(N)}$$

其中,$-\sum p(x)\log(p(x))$为匿名系统熵,$N$ 表示系统中的用户数。

图 4 对比了不同概率下恶意节点占总节点的比例 $C$ 与匿名度之间的函数关系。从图 4 可以看出,随着恶意节点的比例逐渐增大,系统的匿名度不断降低,而且转发概率越大,匿名度也越大。

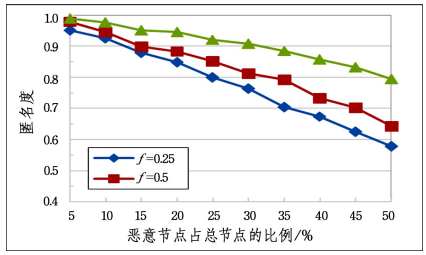


图 4 恶意节点的比例与匿名度的函数关系

Fig. 4 Function relationship of malicious nodes and anonymity

通过上述分析,本文所提出的匿名路由模型可以保证在少量恶意节点存在时,整个通信系统的匿名度达到 0.65 以上。即在预设全部为对等的普通节点的情况下,可以实现较高的匿名度,这也表明本文所提出的基于匿名路由的位置隐私保护可以起到较好的匿名作用。

### 3.3 健壮性分析

本文提出的方案在信息传送过程中不依赖某些特殊节点,网络中任意部分节点的故障都不会影响基于位置的服务正常时限,这是因为该方案是完全自组织、无中心、节点对等的。这种新型的匿名路由模型中,任何一个节点出现问题都不会影响到整个通信过程,即使合谋攻击也无法获得完整的信息传送路线,除非攻击者与移动网络中除了原发送节点和 LBS 服务器的所有节点一起合谋,显然这种情况的概率是极小的。综上,该模型的健壮性较强。当下对移动位置隐私的保护大多从 K 匿名方法出发[14],这种方案的健壮性相对较弱。

### 3.4 通信复杂性分析

对于通信复杂性,在此分析成功建立一条通信路径所需

要的通信复杂度，即在这条成功建立的路径上节点的通信次数。如算法 2 所述，所建立的重路由路径上的中转节点在一定条件下是可以重复的，对于当前的中转节点是不允许发送给自身和上一跳节点的，但是可以发送给上上跳的中转节点。这个模型对转发进行了控制，转发次数大约控制在 9 次以内，在该次数内一定能将查询请求发送到目标服务器。

在请求发送过程中，发送者经过了两层嵌套的对称加密、两次非对称加密过程。中转节点在解密请求包时，只进行一次非对称解密操作和一次对称解密操作。中转节点加密请求包时，进行了一次非对称加密操作和一次对称加密操作。目标服务器在收到请求包时，对数据包进行两次非对称解密操作和两次对称解密操作。目标服务器在发送回复包时，对数据包进行了两层嵌套的对称加密操作，以及一次非对称加密操作。中转节点在处理回复包时的操作复杂度与发送信息包的复杂度等同。初始发送者在接收回复包时进行了一次非对称解密操作和两次对称解密操作。

该匿名路由模型选择固定的转发概率进行重路由路径选择，假设转发概率为 $P_f$，可以计算出路径长度分布为：

$$p(L=k+1)=1\cdot p_f^{k-1}\cdot(1-p_f),1\ll k<+\infty \tag{1}$$

那么转发路径长度的期望值为：

$$E(L)=\sum_{k=1}^{\infty}p_f^{k-1}\cdot(1-p_f)=1+\frac{1}{1-p_f} \tag{2}$$

消息传送失败的概率非常小，大约为 0.78%。具体计算如下：

转发 1 次的成功概率为 $P(X=1)=0$；

转发 2 次的成功概率为 $P(X=2)=1/2$；

转发 3 次的成功概率为 $P(X=3)=(1/2)^2=1/4$；

…

转发 8 次的成功概率为 $P(X=8)=(1/2)^7=1/128$。

那么，在转发次数小于或等于 8 次（$X\leqslant 8$）时，发送成功的概率为：

$$P(X\leqslant 8)=P(X=1)+P(X=2)+P(X=3)+P(X=4)+P(X=5)+P(X=6)+P(X=7)+P(X=8)=127/128\approx 99.22\%$$

因此，转发 8 次后失败的概率为：

$$P(X>8)=1-P(X\leqslant 8)=1-127/128=1/128\approx 0.78\%$$

## 4　实验结果与分析

为了验证基于匿名路由模型的位置隐私保护方法的性能，表 2 列出了实验环境和参数设置。本实验的客户端是在安卓系统的位置服务应用开发基础上实现的。移动手机端和服务器的通信方式采取 socket 连接。

表 2　实验环境及参数设置

Table 2　Experimental environment and parameter setting

| 类别 | 参数 |
|---|---|
| 硬件环境 | CPU:Intel(R)Core(TM)i3 主频:3.40 GHz |
| 操作系统 | Windows 10 Professinal |
| 软件平台 | IntelliJ IDEA 2017.1 x64 |
| 编程语言 | JAVA |
| 匿名节点数需求 | 1,10,20,30,40,50,60,70,80,90,100 |

实验参数定义了平均最大响应时间（$maxTTL$）和平均最小响应时间（$minTTL$），以及平均响应时间（$TTL$）。平均最大响应时间表示当移动网络中 $n$ 个移动节点都在同一时刻发送请求查询消息时，处理一次请求查询操作所用的通信时间。$t_j$ 表示服务器处理第 $j$ 个节点发送一次查询所需要的通信时间。

$$maxTTL=\frac{\sum_{j=1}^{n}t_j}{n} \tag{3}$$

最小平均响应时间表示在移动网络中每个时刻只有一个节点发送地理位置查询信息时，一共发送 $m$ 次请求查询信息，服务器平均处理一次这样的请求操作所用的通信时间。$t_i$ 表示服务器处理某个节点发送的第 $i$ 次请求查询的通信时间。

$$minTTL=\frac{\sum_{i=1}^{n}t_i}{m} \tag{4}$$

平均响应时间（$TTL$）是指，在正常情况下移动网络中节点发送若干次请求，服务器处理单次请求所消耗的通信时间。移动网络中共有 $n$ 个节点，每个节点都在同一时刻发送地理位置查询信息，$x_i$ 表示节点发送的查询次数，$t_{jx_i}$ 表示服务器处理第 $j$ 个节点发送的第 $x_i$ 次查询所需要的通信时间。其中 $\sum_{i=1}^{n}x_i=m,m\neq 0$。$m$ 为 $n$ 个节点一共发送的查询次数。

$$TTL=\frac{(t_{11}+t_{12}+\cdots+t_{1x_i})}{\sum_{l=1}^{n}x_i}+\frac{(t_{21}+t_{22}+\cdots+t_{2x_i})}{\sum_{i=1}^{n}x_i}+\cdots+\frac{(t_{n1}+t_{n2}+\cdots+t_{nx_m})}{\sum_{i=1}^{n}x_i}=\frac{\sum_{j=1}^{n}\sum_{i=0}^{n}t_{jx_i}}{\sum_{i=1}^{n}x_i} \tag{5}$$

图 5 给出了在转发概率为 1/2 时，移动节点数目逐渐增加的情况下的平均最大响应时间、平均最小响应时间和平均响应时间的变化情况。从图 5 中可以看出平均时延在 100 个移动节点组成的网络中的时间最多不超过 40 s，低于平均最大时延。平均最大时延在真实的环境中出现的情况是较少的，即网络中所有移动节点在同一时刻提出地理位置查询信息的情况。平均最小时延一直比较稳定，大约保持在 10 s 内，因此响应速度较快，这与转发路径的长度有很大的关系。可以得出这样的结论：随着节点数量的不断增长，平均响应时间基本呈线性增长，并未出现随着节点数量增长，平均响应时间指数上升，导致网络通信陷于瘫痪的情况。这表明即使在移动客户端并发访问量很大的情况下，该方案仍然适用且具有较好的稳定性和健壮性。

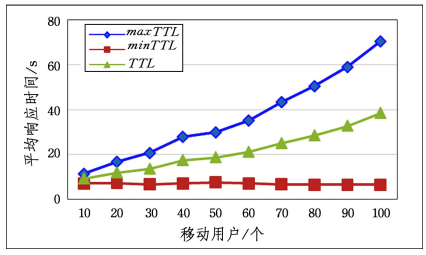


图 5　通信时间

Fig. 5　Communication time

图 6 是在 100 个移动节点组成的网络中进行信息转发，模拟进行 50 次实验后得到的转发路径长度变化图。可以看出，随着实验次数的增多，节点的转发路径长度呈现平稳趋势，最后稳定在一个固定的数值附近。这表明转发路径长度与历史实验次数无关，即在信息传送的过程中不存在利用历史路径转发信息的情况，这也保证了移动节点在每次发送地理位置查询信息时，信息传送路径都是随机产生的，保证了移动节点位置的匿名安全性。

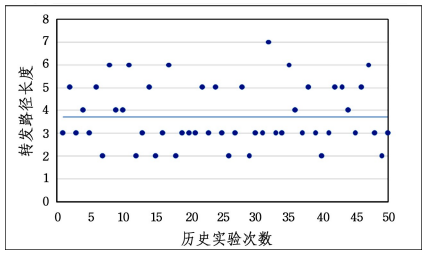


图 6 转发次数

Fig. 6 Frequency of forwarding

图 7 表示不同概率和不同移动节点数量下，地理位置查询信息的转发路径长度。实验的具体操作过程是在控制转发概率分别为 0.25，0.5，0.75 的情况下，分别在 5，10，15，20，…，100 个移动节点组成的网络中进行信息转发，分别模拟进行 100 次实验，记录在不同移动节点组成的网络中的路径长度，得到如图 7 所示的平均路径长度变化图。随着移动网络节点数的逐渐增多，信息的平均转发路径长度没有大幅度变化，都是在某个恒定值上下波动，波动范围不超过 2。这表明平均转发路径长度与网络中的节点个数是无关的。这同样表明了该方案的稳定性，即在移动节点较多的网络中使用该方案不会影响信息的传输性能。

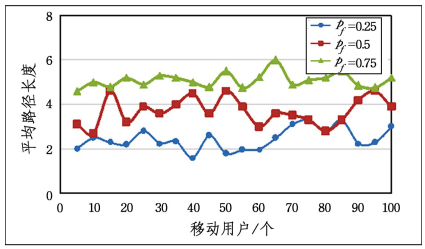


图 7 平均路径长度

Fig. 7 Average path length

从图 7 中还可以看出，在不同的转发概率下，平均路径长度是不同的。随着转发概率的增大，平均路径长度也在增加，这与上文的理论分析一致。在转发概率为 3/4 时，平均路径长度最长，大约为 5；在转发概率为 1/4 时，平均路径长度最短，大约为 2.5。通信路径过短时，攻击者可能通过流量分析攻击方式推断出用户的身份信息[18]；通信路径过长时，用户在获取基于位置的服务时的时延就会较大，不利于用户体验。因此，本文匿名路由模型选取转发概率为 1/2，在保证移动节点位置隐私的前提下，以较低的时延进行通信。

**结束语** 本文采用 AES 算法与 RSA 算法相结合的方式对查询信息混合加密，在传送过程中以 1/2 的概率随机选择若干中间节点，传送过程中的路径长度是不确定的。全部参与信息传递的节点只知道前驱节点与后继节点，保护了移动发送节点的位置隐私。并且经过实验验证，该匿名路由模型的时延很小，健壮性强，能够很好地避免由于信息量增多导致的网络拥塞的情况。

未来将在实际环境更复杂的情况下对模型效率做进一步的提升，从而达到使通信网络更加灵活、安全的目的。

## 参 考 文 献

[1] SHIN K G，JU X，CHEN Z，et al. Privacy protection for users of location-based services[J]. Wireless Communications IEEE，2012，19(1)：30-39.

[2] CHAUM D L. Untraceble electronic mail，return addresses，and digital pseudonyms[J]. Communications of the ACM，1981，24(2)：84-88.

[3] SYVERSON P F，GOLDSCHLAG D M，REED M G. Anonymous Connections and Onion Routing[C]// IEEE Symposium on Security and Privacy. IEEE Computer Society，1997：44.

[4] DINGLEDINE R，MATHEWSON N，SYVERSON P. Tor：the second-generation onion router[C]// Conference on Usenix Security Symposium. USENIX Association，2004：21.

[5] RELTER M K，RUBIN A D. Crowds：A nonymity for web Transactions[J]. ACM Transactions on Information and System Security，1998，1(1)：62-92.

[6] PENG Z Y，LI S P. Protecting Location Privacy in Location-based Services in Mobile Environments[J]. Journal of Electronics & Information Technology，2011，33(5)：1211-1216.(in Chinese)
彭志宇，李善平. 移动环境下 LBS 位置隐私保护[J]. 电子与信息学报，2011，33(5)：1211-1216.

[7] SWEENEY L. k-ANONYMITY：A Moedl for Protecting Privacy[J]. International Journal of Uncertainty，Fuzziness and Knowledge-Based Systems，2002，10(5)：557-570.

[8] LUO J，LIAO J G，LI X. LocPriv：a Scheme on Location Privacy Protection Based on Spatial Region Anonymity[J]. Smallmicrocomputer Submission，2016，37(6)：1273-1278.(in Chinese)
罗健，廖俊国，李雄. LocPriv：一种基于空间区域匿名的位置隐私保护方案[J]. 小型微型计算机系统，2016，37(6)：1273-1278.

[9] GKOULALAS-DIVANIS A，KALNIS P，VERYKIOS V S. Providing K-Anonymity in location based services[J]. ACM，2010，12(1)：3-10.

[10] XU H Y，XU J GONG Y J，et al. Algorithms to Generate Location Privacy Protection with Spatial Cloaking[J]. Journal of South China University of Technology(Natural Science Edition)，2014，42(1)：97-103.(in Chinese)
徐红云，许隽，龚羽菁，等. 基于空间混淆位置隐私保护的位置隐私区域生成算法[J]. 华南理工大学学报(自然科学版)，2014，42(1)：97-103.

[11] KHOSHGOZARAN A，SHAHABI C. Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy[C]// International Conference on Advances in Spatial and Temporal Databases. Springer-Verlag，2007：239-257.

[12] LIU X J，CHEN Y F，LI B. Mobile Location Privacy Protection

Based on Untrusted Environment[J]. Computer Science, 2015, 42(2): 108-113. (in Chinese)
刘学军，陈玉凤，李斌. 基于不可信环境的移动位置隐私保护[J]. 计算机科学，2015，42(2)：108-113.

[13] HUO Z, MENG X F. A Surey of Trajectory Privacy-Preserving Techniques [J]. Chinese Journal of Comuputers, 2011, 34(10): 1820-1830. (in Chinese)
霍峥，孟小峰. 轨迹隐私保护技术研究[J]. 计算机学报，2011，34(10)：1820-1830.

[14] MENG X F, PAN X. Privacy Preservation based on Location Services[J]. Communications of the CCF, 2010, 6(6): 16-23. (in Chinese)
孟晓峰，潘晓. 基于位置服务的隐私保护[J]. 中国计算机协会通讯，2010，6(6)：16-23.

[15] HUANG X H. Research on Location Privacy Preservation in Location-based Services[D]. Chengdu: University of Electronic Science and Technology of China, 2016. (in Chinese)
黄勋辉. 基于位置服务的位置隐私保护研究[D]. 成都：电子科技大学，2016.

[16] SEN S, WANG J. Analyzing peer-to-peer traffic across large networks[J]. IEEE/ACM Transactions on Networking, 2004, 12(2): 219-232.

[17] REITER M K. Crowds: anonymity for Web transactions[J]. Acm Transactions on Information & System Security, 1998, 1(1): 66-92.

[18] DIAZ C, CLAESSENS J, PRENEEL B. APES: Anonymity and Privacy in Electronic Services[J]. Datenschutz Und Datensicherheit, 2005, 27(3): 143-145.

(上接第 123 页)

扰的能力。同时控制次网的用户数对整个系统的天线效率也有增益效果。本文通过分析给出该模型的最佳天线配置，提高了系统的天线效率。下一步工作是将本方案应用到其他并存模型中，使更多的单广播网络并存，以适应当下不同场合的需要。

## 参 考 文 献

[1] BIGLIERI E, CALDERBANK R, CONSTANTINIDES A, et al. MIMO wireless communications [J]. Cambridge University Press, 2007, 51(11): 2709.

[2] VISHWANATH S, JINDAL N, GOLDSMITH A. Duality, achievable rates, and sum-rate capacity of Gaussian MIMO broadcast channels [J]. IEEE Transactions on Information Theory, 2003, 49(10): 2658-2668.

[3] WANG Y, LIU F, ZENG L S, et al. Analysis of KusersBC network with null space intersection and Multicast[J]. Journal of Xidian University (Natural Science Edition), 2018, 45(2): 135-140. (in Chinese)
王越，刘锋，曾连荪，等. 结合零空间交与多播的 K 用户 BC 网络分析[J]. 西安电子科技大学学报(自然科学版)，2018，45(2)：135-140.

[4] CHEN J Y, ELIA P. MIMO BC with imperfect and delayed channel state information at the transmitter and receivers [C]// 2013 IEEE 14th Workshop on Signal Processing Advances in Wireless Communications (SPAWC). 2013: 195-199.

[5] STAVRIDIS A, RENZO M D. Performance Analysis of Multistream Receive Spatial Modulation in the MIMO Broadcast Channel[J]. IEEE Transactions on Wireless Communications, 2016, 15(3): 1808-1820.

[6] LEE N, SHIN W, HEATH R W, et al. Interference Alignment with limited feedback for two-cell Interfering MIMO-MAC [C]// International Symposium on Wireless Communication Systems (ISWCS). IEEE, 2012: 566-570.

[7] JAFAR S A, FAKHEREDDIN M J. Degrees of freedom for the MIMO interference channel [J]. IEEE Transactions on Information Theory, 2007, 53(7): 2637-2642.

[8] CHEN G, XIANG Z, XU C, et al. On Degrees of Freedom of freedom of wireless X networks [J]. IEEE Transactions on Information Theory, 2009, 55(9): 3893-3908.

[9] IGHOMI M Z, WANG Z D. Degrees of Freedom Region of Wireless X Networks Based on Real Interference Alignment [J]. IEEE Transactions on Information Theory, 2016, 62(4): 1931-1941.

[10] PIZZIO R, UCHÔA-FILHO B F, RENZO M D, et al. Generalized spatial modulation for downlink multiuser MIMO systems with multicast [C]// 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). NJ: IEEE Press, 2016: 1-6.

[11] CHOI Y I, KANG C G. MIMO transmission scheme for scalable video broadcast and multicast service [C]// 2016 International Conference on Information and Communication Technology Convergence (ICTC). NJ: IEEE Press, 2016: 365-367.

[12] JO G, LEE J N, BAE H O, et al. LTE based spatialmultiplexing MIMO with single radio[C]// 2016 46th European Microwave Conference (EuMC). IEEE, 2016: 1319-1322.

[13] YANG L, QARAQE K, SERPEDIN E, et al. Sum-rate analysis of spectrum sharing spatial multiplexing MIMO systems with zero-forcing and multiuser diversity [C]// 2013 IEEE 14th Workshop on Signal Processing Advances in Wireless Communications (SPAWC). 2013: 585-589.

[14] MOHARRAM M A, KISHK A A. MIMO Antennas Efficiency Measurement Using Wheeler Caps [J]. IEEE Transactions on Antennas and Propagation, 2016, 66(3): 1115-1120.

[15] REN H, LIU N, PAN C H, et al. Energy Efficiency Optimization for MIMO Distributed Antenna Systems[J]. IEEE Transactions on Vehicular Technology, 2017, 66(3): 2276-2288.

[16] 张贤达. 矩阵分析与应用(第二版)[M]. 北京：清华大学出版社，2004：601-613.