移动互联网络动态匿名算法设计与分析

见晓春[1],吴振强[1,2],王小明[1],霍成义[1],张 婕[1]
JIAN Xiao-chun[1],WU Zhen-qiang[1,2],WANG Xiao-ming[1],HUO Cheng-yi[1],ZHANG Jie[1]

1.陕西师范大学 计算机科学学院,西安 710062
2.西安电子科技大学 计算机网络与信息安全教育部重点实验室,西安 710071
1.College of Computer Scienc,Shaanxi Normal University,Xi'an 710062,China
2.The Ministry of Education Key Lab of Computer Networks and Information Security,Xidian University,Xi'an 710071,China

JIAN Xiao-chun,WU Zhen-qiang,WANG Xiao-ming,et al.Design and analysis of dynamic anonymity algorithm in mobile Internet.Computer Engineering and Applications,2009,45(18):115-119.

Abstract: This paper presents an anonymity algorithm,which dynamically changes source address in IP layer to make a anonymity communications.In sending packet,it dynamically establishes the anonymity link,while encrypting and recording the middle address in packet.The record of middle addresses on the path is encrypts hop by hop,which looks like a onion with the source IP inside and destination IP outside.The response of the packet traces the middle address back to the original source node.The algorithm does not only ensuring the sender anonymous,but also protecting the information of the source address from lost.Analysis shows that the algorithm can provide high-level anonymous,dynamically ensconce the source address,has less bandwidth cost,has less encryption times and shorter time delay.So the algorithm can provide high quality anonymity communication in IP layer in mobile Internet.

Key words: security of data and computer;anonymity algorithm;dynamically change source address;encrypt mid-address;sender anonymity

摘 要: 提出了一种匿名算法,通过在IP层动态变化源地址,实现匿名通信。该算法在发送报文时动态建立匿名链路,加密记录中间结点地址,形成一个源地址在最内层,最后一跳节点地址在最外层的洋葱地址数据。在报文应答时,按照发送时形成的洋葱地址数据逐跳回送应答报文。这样既有效保证了发送方匿名,又保证了源地址信息不丢失。分析表明,该算法动态隐藏源地址,匿名度高,带宽消耗低,加解密次数少,时延短,可以为移动互联网络提供优质的网络层匿名通信服务。

关键词: 数据安全与计算机安全;匿名算法;动态替换源地址;加密中间结点;发送方匿名
DOI: 10.3778/j.issn.1002-8331.2009.18.035 **文章编号:** 1002-8331(2009)18-0115-05 **文献标识码:** A **中图分类号:** TP393.08

1 引言

随着信息网络技术的快速发展,促使Internet从无线互联网络(Wireless Internet)向无线移动互联网络(Wireless Mobile Internet,WMI)[1]的演化。据分析,移动互联网络有其新的特点,动态变化的拓扑结构;开放的链路;有限的带宽和计算资源。这些特征使消息更容易被截获和监听,移动互联网络面临更多安全威胁[2]。现有的加密技术可以保护消息内容的安全性,但是敌手仍然可以通过获得通信双方的报头信息,例如源地址和目的地址、报文长度来推断信息的来源、去向、数据量和一些隐含的意义,进而间接获得通信者的网络位置、身份甚至所在局域网结构。随着一些特殊部门,例如军事、国防、政府部门对移动互联网络安全要求的提高,以及民用上对移动互联网络个人隐私要求的提高,迫切要求在移动互联网络进行匿名通信。匿名技术通过一定的方法将通信流中的通信关系加以隐藏,使攻击者无法获知双方的通信关系或通信的一方。移动互联网络上匿名算法能够适应多变的网络拓扑结构,系统开销小,效率高。

现有的匿名系统主要集中在有线网络中,可以提供无关联性匿名的技术有广播技术、代理技术和混淆技术三大类。其中广播技术有广播隐式地址(Implicit Addresses)法[3-4]和DC网络法(Dining Cryptographers Network)[5],这两种方法要求系统的参与方在一个封闭的匿名集合中,无法适应开放式的移动互联网络;单代理技术有Anonymizer[6]和Lucent[7],Anonymizer虽然在移动环境下位置隐私的保护[8-9]上有所应用,Lucent是Anonymizer在基础上自动生成假名,但是攻击者仍能根据节点的出入消息建立相应的映射关系而威胁系统的匿名性;多代理Crowds[10]及洋葱路由(Onion Routing)[11]采用重路由机制使其负

基金项目: 国家自然科学基金(the National Natural Science Foundation of China under Grant No.60503008)。
作者简介: 见晓春(1983-),女,硕士生,研究方向为网络和信息系统安全;吴振强(1968-),男,副教授,硕士生导师,主要研究方向为移动互联网络和匿名通信;王小明(1964-),男,教授,博士生导师,主要研究方向为信息系统安全、访问控制和数据库;霍成义(1972-),男,硕士生,研究方向为网络和信息系统安全;张婕(1981-),女,硕士生,研究方向为网络和信息系统安全。
收稿日期: 2008-04-15 **修回日期:** 2008-07-18

载代价较大,不适合移动互联网。Chaum 在 1981 年提出的混淆(Mix)技术[12]是采取重新排序、延迟和填充等方法来加大攻击者流量分析的难度,这种技术对网络带宽消耗较大。文献[13]针对 Ad Hoc 网络改进了混淆(Mix)方法,提出了动态混淆方法 DMM(Dynamic Mix Method),该方法的核心是动态选择混淆节点(mix nodes)。通过 CM(Closest Mix)协议选择最近的混淆节点,用 OM(Optimal Mix)协议选择整体路径最优的混淆节点。该方法的不足之处是作者还没有提出混淆节点的发现算法,只给出了发现混淆节点之后的选择方案,因此其可用性在发现算法成熟后,才有现实意义。文献[14]提出了一种 Ad Hoc 网络动态混淆的 RM(pseudo-Random Mix)算法,该算法主要对混淆器的管理部分进行重新设计。RM 算法根据混淆缓冲区的情况进行决策,当缓冲区未满时采用时延转发方式,缓冲区满时采用随机数转发方式,但是此方法沿用了有线网络下的固定混淆节点,在移动互联网下寻找混淆节点耗时耗力。

提出了源地址动态变化匿名算法。这一算法首先,将源地址动态变化为多个伪装地址从而实现了发送方匿名(sender anonymity)。其次,将真正的源地址和整个链路上中间节点一起层层加密,携带在 IP 报文中,支持 IP 报文匿名应答。本文算法匿名度较高,系统开销小,几乎不影响网络带宽,特别适合移动互联网络环境。

2　源地址动态变化匿名算法设计与实现

源地址动态变化匿名算法针对移动互联网多变的拓扑结构,有限的计算资源,开放的链路等特点提出,因此,对它的使用环境做如下假设:(1)网络内各节点,不论是端节点还是路由节点都是可编程的,能够加载本文提出的算法处理程序。(2)网络内各节点,具备公钥密码协议,且其是安全的。(3)报文内容已经进行端到端加密,能保证其内容的机密性。(4)移动互联网采用多路径路由寻址方法。

2.1　源地址动态变化匿名算法思想

源地址动态变化匿名算法,核心思想是:首先,利用移动互联网络已有的多路径路由将 IP 数据包从源节点向目标节点发送,在每个中间节点,把源地址修改为本节点的地址再转发。从而源地址在每个中间节点都动态变化,目标节点收到的 IP 报文源地址是某个中间节点的地址。其次,为了不丢失源地址信息,为了能够将 IP 报文的应答消息回发给源节点,要把从源到目标的地址及途经的中间结点地址,层层用各节点的公钥加密形成一个地址洋葱数据块,并把这个洋葱地址数据块携带在 IP 报文当(洋葱地址数据块的形成将在 2.2 节中详细说明)。再次,如果该 IP 报文需要发送应答报文给源发送方,则应答报文携带洋葱地址数据块原路返回,在每个中间节点解密洋葱地址数据块,得到下一跳节点地址,直至源发送方。

图 1 举出了有 4 个结点时的发送和回送过程中的 IP 报文信息变化过程。其中,IP_A 表示源发送端 A 的 IP 地址;$E_B(IP_A)$表示用非对称加密,对 A 点的 IP 地址用 B 点的公钥加密;‖是拼接运算,表示前面的字串拼接后面的字串成为一个新字串;$c1$ 表示第一个 IP 报文在洋葱地址数据块中存储的内容。

2.2　洋葱地址数据块的形成过程

为了支持 IP 报文匿名应答,动态变化源地址匿名算法中的目标节点,收到的报文中需要挟带源地址真实信息。为了解决这个问题,存储从源到目的中间结点,把这些从源到目的的

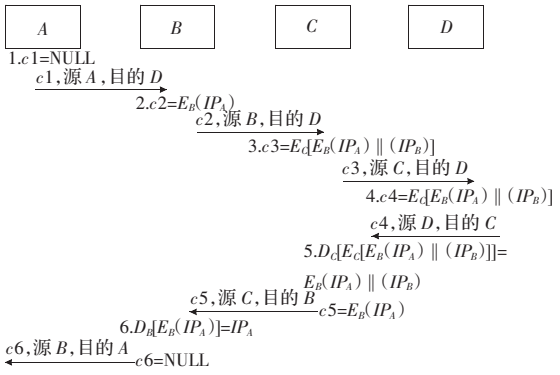

图 1　4 个节点时 IP 报头信息变化

中间结点逐跳加密封装成一个源地址在最内层,第一跳地址在次内层,最后一跳地址在最外层的层次结构。这种地址记录格式类似洋葱路由技术中的洋葱路由数据包,因此,称为洋葱地址数据块。需要注意的是,这个洋葱路径记录数据块和洋葱路由有质的区别。首先,本文的洋葱地址数据块是正向记录中间节点的,而洋葱路由是反向生成路由中间的节点。其次,本文的洋葱地址数据块每层加密,使用中间结点本身公钥,而洋葱路由是用下一个节点的公钥加密,所以本文算法不涉及密钥交换,大大提高了效率。再次,本文的洋葱地址数据块在对中间路由节点地址加密,而洋葱路由对整个消息加密。

图 2 给出了 WLAN-WMAN-Internet 三级结构移动互联网中,洋葱地址数据块生成过程示意图。随着移动互联网络链路的建立和移动路由,从源地址到目标地址的中间节点将顺向层层加密成一个洋葱。其中,每层都在原洋葱地址数据块上拼接一个上一中间节点地址,这个整体在用本节点的公钥加密。如果,IP_A 表示源发送端 A 的 IP 地址;$E_B(IP_A)$表示用非对称加密,对 A 点的 IP 地址用 B 点的公钥加密;‖是拼接运算,表示前面的字串拼接后面的字串成为一个新字串;则每个洋葱路径记录块记录的信息如下:

第一个节点(A,即发送方)洋葱地址数据:NULL

第二个节点(B)洋葱地址数据:$E_B(IP_A)$

第三个节点(C)洋葱地址数据:$E_C[E_B(IP_A) \| (IP_B)]$

第四个节点(D)洋葱地址数据:$E_D[E_C[E_B(IP_A) \| (IP_B) \| (IP_C)]$

……

第 $X+1$ 个节点洋葱地址数据:$E_{X+1}[\cdots \wedge E_D[E_C[E_B(IP_A) \| (IP_B) \| (IP_C) \| \wedge \cdots (IP_X)]$

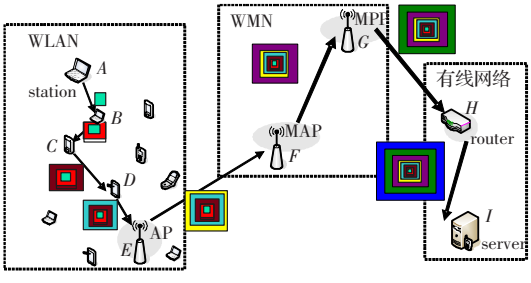

图 2　洋葱地址数据的形成过程

2.3　中间节点匿名处理流程

为了实现本算法,网络内各节点,不论是端节点还是中间路由节点都是可编程的,能够加载本文提出的算法处理程序。该程序流程如图 3 所示。首先获取 IP 报文,先判断其是否标记

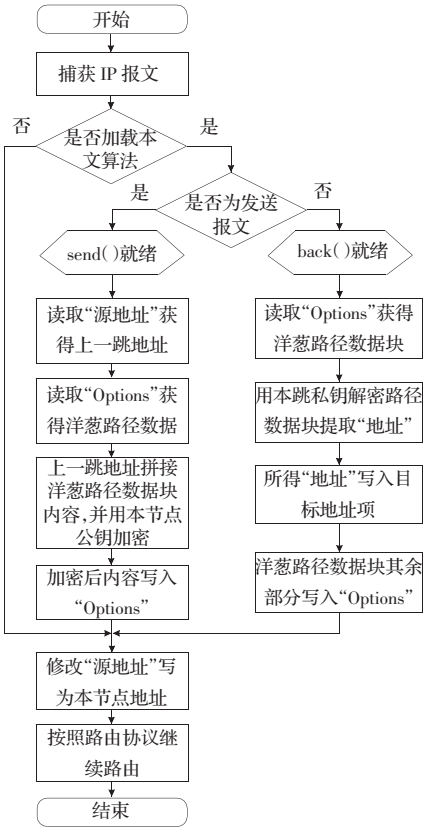

图 3　IP 报文在中间节点上处理流程

为使用提出的匿名算法,如该 IP 报文执行本文算法,且为发送报文,则转到发送进程 send( );如该 IP 报文执行本文算法,且为应答报文,则转到回送进程 back( );没有使用本文提出的匿名算法则按照网段上的路由协议直接路由。进程 send( )负责处理从由 station 到 server 的发送报文。它首先将网络层的 IP 报文捕获,将报文源地址提取出来按照 2.2 节中的算法加密形成新的洋葱地址数据,再把源地址修改为本节点地址,IP 报文按网络路由协议继续路由,直到目标节点 server。进程 backtrack( )负责处理从 server 到 station 的应答报文。它首先将网络层的 IP 报文捕获,用本节点的私钥解密洋葱地址数据,得到最前面拼接的下一跳节点地址,把它的值写入目标地址,把本节点的地址写入源地址,IP 报文按路由协议继续路由,直到源节点 station。

2.4　IP 报文填充

为了实现本文算法,要把涉及到的报头信息填充到在现有的IPv4 报头结构中。图 4 是 IP v4 报头结构,本文的算法涉及服务类型,源地址,目的地址和选项(Options,可变长字段)。首先,服务类型(8 bit)中,还预留了后 2 位(IP 报头的第 14,第 15 位)没有使用,使用这两位来做标记:第 14 位置 1,则为使用本文算法的 IP 报文,否则普通 IP 报文。第 15 位置 1,则为发送报文,否则为回送报文。其次,本算法在路由的每一跳都修改源 IP 地址(32 bites)和目标 IP 地址(32 bites)。再次,用洋葱地址数据块填充选项(Options,可变长任意字段)。选项字段是可变长的,长度是 0~10 个 32 位字,因此洋葱地址数据块最多可以存储 10 个中间节点地址。

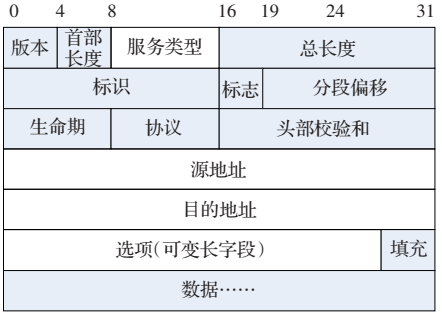

图 4　IPv4 报头信息填充位置

3　分析

3.1　匿名度分析

C.Shields 和 B.N.Levine 对匿名性给出比较精确的定义[15]。设请求方实体 x 与响应方实体 e 的连接概率是 $pr_e(x)$,其中 x 是非空集合 S 的成员,根据概率特性,对不同的 x,将会有 $\sum_{x\in S} pr_e(x)=1$,然而攻击者通过全程分析可以打破这种等概率性。设实体 x 与通信相对的另一个实体 e 在指定的匿名协议 A 下的匿名度定义为:

$$d_{x,e}(A)=\sum_{y\in S\neq x} pr_e(y) \tag{1}$$

与之等价的等式为 $d_{x,e}(A)=1-pr_e(x)$。如果 S 中所有成员以相等的概率进行初始化一个连接,那么

$$d_{x,e}(A)=1-1/|S| \tag{2}$$

移动互联网多通过无线连接,受信号强度和自组织性的影响,一个结点可能与相邻的多个节点进行无线连接,大部分的结点连接度保持在一定数目,符合钟形曲线,因此其网络连接的拓扑结构近似为随机网络。对于在链路上侦听到的 IP 报文,只能看到是本节点发给目标节点的报文,而真正的发送方是什么呢,敌手需要向前倒推源地址。倒推的所有可能是发送方的节点形成匿名集合。为了分析上的不重不漏,把倒推的有向的网络拓扑图转换成与之相对应的有向生成树, 如图 5 所示,根节点是被侦听的节点,孩子节点是可以向父结点发送报文的所有节点。

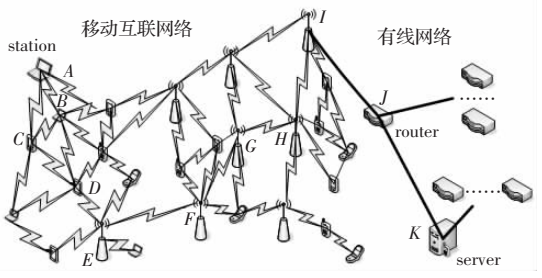

图 5　某被监听网段

有向生成树是网络拓扑结构的抽象,指一棵树,其每个节点的孩子节点对该节点有向可达且方向指向该节点。假设 I 节点的报文被侦听,要倒推发送方,则需要分析的有向生成树为从 I 向下的子树。发送方可能是这棵有向生成树上的所有节点,匿名集合就是这棵树上的所有节点,如图 6 所示。

由于移动互联网络中大部分节点的连接度保持在一定数目,设每个节点可以借收来自 N 个节点的数据,取网络中第 i 个节点的入度为 N_i,入度期望值为 $E(N)$。第 j 个报文从源发送方到接收方经过 L_j 个中间结点,链路长度期望值为 $E(L)$。简化这个模型,把有向生成树抽象为高度为 $E(L)$的满 $E(N)$叉树,

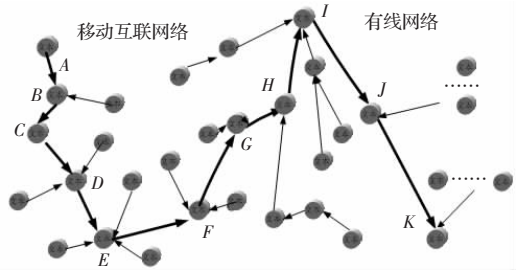

图 6 被监听网段的入度树

这棵树上的所有节点都有可能是发送方。匿名集合大小是有向生成树上的所有节点的数目 S。根据树的性质知,高度为 K 的满 N 叉树的所有节点数目为:

$$\frac{N^{K+1}-1}{N-1} \tag{3}$$

其中 K 为树的高度,单独一个节点为 0 层;N 为节点的度,也是其每个节点孩子的个数。把 $E(L)$和 $E(N)$代入式(3),匿名集合大小为:

$$S=\frac{E(N)^{E(L)+1}-1}{E(N)-1} \tag{4}$$

由于 S 中所有成员以相等的概率进行初始化一个连接,即有向生成树上的每个节点,以等概率连接其父节点。把式(4)代入式(2),得到实体 x 在本文算法下的匿名度随结点入度 $E(N)$ 和链路长度 $E(L)$的变化函数。

$$d_{x,e}(A)=1-\frac{1}{\left|\frac{E(N)^{E(L)+1}-1}{E(N)-1}\right|} \tag{5}$$

在 MATLAB 里对上式得出的匿名度进行分析。当链路长度期望 $E(L)$从 1 到 10 变化,节点平均入度期望 $E(N)$从 2 到 50 变化,匿名度随这两者变化如图 7 所示。通过图 7 的曲面可以看出,本文算法的匿名度随 $E(L)$和 $E(N)$的增大而增大,受 $E(L)$的影响较大。在 $E(L)\geqslant 1$,$E(N)\geqslant 2$ 的情况下,匿名度在 0.75 到 1 之间分布,且在 $E(L)\leqslant 4$,$E(N)\leqslant 20$ 以内快速增大,在 $E(L)\geqslant 4$,$E(N)\geqslant 20$ 以上已经基本趋近于 1。

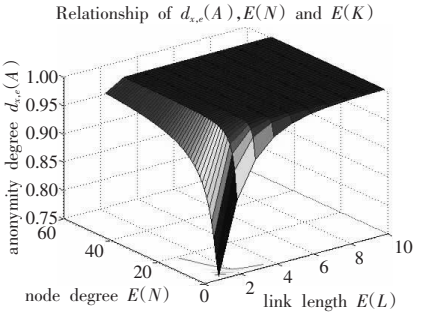

图 7 匿名度随和的变化

根据 Reiter 和 Rubin 对匿名度的分类[16],以及文献[17]匿名分级量化定义:

5 级匿名,即完全暴露(provably exposed),当攻击者可以证明发送者的角色 x(或接收者的角色 e)时,5 级匿名定义为 $d_{x,e}(A)=0$。

4 级匿名,即部分暴露(exposed),存在角色 x 不是发送者(或接收者 e)的可能且满足 $0<d_{x,e}(A)<0.5$,4 级匿名定义为 $d_{x,e}(A)\in(0,0.5)$。

3 级匿名,即可能清白(possible innocence),角色 x 是否为发送者(或接收者 e)的概率相当,但与其他实体相比,有更高的概率可能 $0.5\leqslant d_{x,e}(A)<d_{y,e}(A)$,且 $d_{x,e}(A)<1-1/|S|$,$\forall y\neq x\in S$。则 3 级匿名定义为 $d_{x,e}(A)\in(0.5,1-1/|S|)$。

2 级匿名,即超出猜测(beyond suspicion),角色 x 是发送者(或接收者)的概率不比系统中其他角色有更高的可能。$|S|>2$,$1-1/|S|\leqslant d_{x,e}(A)$,且 $d_{y,e}(A)\leqslant d_{x,e}(A)$,$\forall y\neq x\in S$。则 2 级匿名定义为 $d_{x,e}(A)\in[1-1/|S|,1)$。

1 级匿名,即绝对匿名(absolute anonymity),攻击角色 y 不能获取通信角色 x 的任何证据;当 $|S|\to\infty$ 时,$d_{x,e}(A)=1$。则 1 级匿名定义为 $d_{x,e}(A)=1$。

在本文算法中,$d_{x,e}(A)\in[0.75,1)$,由等概率连接 $d_{x,e}(A)+d_{y,e}(A)=1$,得 $d_{y,e}(A)\in(0,0.25]$。可见,本文算法满足 $|S|>2$,$1-1/|S|=d_{x,e}(A)$,且 $d_{y,e}(A)\leqslant d_{x,e}(A)$,$\forall y\neq x\in S$。综上,算法达到 2 级匿名,即超出猜测(beyond suspicion),随 K 和 N 的增大,甚至接近完全隐私。

图 8 详细放大了图 7 曲线在底面上的 5 条等值线投影,给出了 $d_{x,e}(A)=0.75$,$d_{x,e}(A)=0.80$,$d_{x,e}(A)=0.85$,$d_{x,e}(A)=0.90$,$d_{x,e}(A)=0.95$ 几个量化匿名度的等值线及相应的 $E(L)$和 $E(N)$的取值范围。

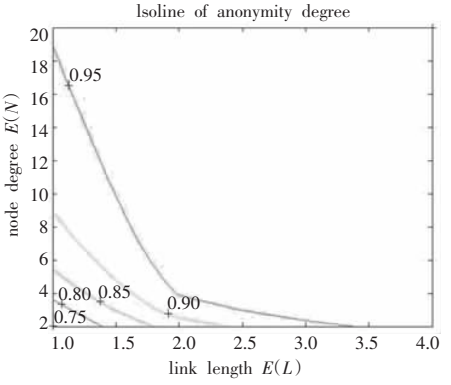

图 8 匿名度的等值线

3.2 性能分析

鉴于 Crowds 和 Onion Routing II 是目前有线网络上较先进成熟的匿名算法,移动网络上尚无成熟的匿名算法,并且本文的算法是基于路由的,类似于重路由系统,所以本文以Crowds 为对比对象,分析算法的性能。目前 Crowds 和 Onion Routing II 采用的是如下重路由策略:从系统 n 个成员(包括发送者自身)随机选取节点作为重路由路径上的中继结点,路径长度 L(把发送者和代理节点个数作为其重路由路径长度)为服从某一概率分布的离散随机变量。下面分析以在同一段移动互联网络中发起一次数据量相同的匿名通信为场景。

3.2.1 链路长度

从应用层看,在 Crowds 通过多个中间代理实现重路由,每个代理是它的中继节点。Reiter 等把发送方计入路径长度,文献[18]给出 Crowds 重路由路径长度的数学期望为 $E(Lm)=1/(1-p_f)+1$,$(0.5\leqslant p_f<1)$。其中 p_f 表示 Jondo 随机选取一个 Jondo 作为后继,并将请求转发给该后继 Jondo。当后继 Jondo 获得请求,以概率 $p_f(0.5\leqslant p_f<1)$将请求继续转发,否则将请求直接提交给接收者。本文算法从源发送节点到目标节点不经过应用层代理,因此可以看作重路由路径长度为 1。

从网络层看,设每个节点可以借收来自 N 个节点的数据,取网络中第 i 个节点的入度为 N_i,入度期望值为 $E(N)$。第 j 个报文从源发送方到接收方经过 L_j 个中间结点, 链路长度期望

值为 $E(L)$。在 Crowds 系统中,发送方到接收方的重路由长度为 Lm,每两个 Jondo 代理之间有 X_i 条路由路径,分别经过长度为 L_j 的路径到达。在移动互联网络内其数学期望分别为 $E(Lm)$,$E(X)$和 $E(L)$。因此,Crowds 系统从发送方到接收方总的路径长度期望为:$E(L_{crowds})=E(Lm)\times E(X)\times E(L)$。

本文的算法从发送方到接收方之间有 X_i 条路由路径,分别经过长度为 L_j 的路径到达。因此,本文算法从发送方到接收方总的路径长度期望为:$E(L_{new})=1\times E(X)\times E(L)$。

在同一网络内,不论使用 Crowds 还是本文算法,$E(X)$和 $E(L)$总是特定的值的,为了将提出的算法和 Crowds 对比,令 $E(X)\times E(L)=a$。则

$E(L_{new})=1\times a$

$E(L_{crowds})=[1/(1-p_f)+1]\times a,(0.5\leqslant p_f<1)$

在 Matlab 里以 a 的倍数为标度分析对比随转发概率变化。

由图 9 可见,算法的总链路长度代价是 $1a$,Crowds 重路由系统链路长度从 $3a$ 开始随转发概率 p_f 增大而增大。算法的总链路长度代价远低于 Crowds 重路由系统。受此影响,算法的网段内数据流量,带宽消耗远小于 Crowds 等重路由系统。

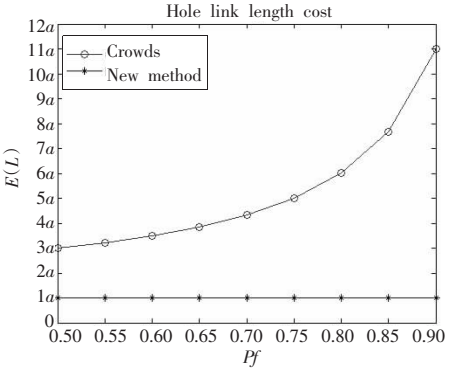

图 9 总链路长度代价比较

3.2.2 加解密处理代价

Crowds 等重路由系统在每个代理节点上进行,每个节点进行一次解密和一次加密,记为 2,则一次通信共进行加解密次数为 $2\times[1/(1-p_f)+1]$。算法中,加解密在每个路由节点上进行,每次进行一次解密或者一次加密,记为 1,则通信共进行加解密次数为 $E(X)\times E(L)$,其中 $E(L)$的上限是 10。具体数值大小依赖于所选的移动互联网络段的网络特征,但是大部分时候本文算法的加解密次数少于 Crowds 重路由系统。本文算法不需要交换密钥,Crowds 等重路由系统需要交换密钥。

3.2.3 时延

系统总时延=链路传输时延+节点处理时延

节点处理时延主要体现在各路径不可并行处理的加解密时延。Crowds 等重路由系统加解密是现行后继的关系,所以每次加解密都不可并行。设执行一次加解密时延为 t,则一次通信共进行加解密时延为 $2t\times[1/(1-p_f)+1]$,其中$(0.5\leqslant p_f<1)$。在 $p_f\geqslant 0.75$ 时,加解密时延 $\geqslant 10t$;在算法中多路径路由可以同时进行,因此 $E(X)$条路由路径可以并行加密。由于需要加解密的链路长度 $E(L)$上限是 10,即每个路径加解密最长 10 个节点。所以一次通信中的加解密时延为 $t\times E(L)$,$1\leqslant E(L)\leqslant 10$。加解密时延 $\leqslant 10t$。所以,Crowds 等重路由系统在 $p_f\geqslant 0.75$ 时,算法节点时延恒小于 Crowds 等重路由系统时延。由于 Crowds 等采用重路由,而算法一次路由即可,所以,算法连路传输时间小于 Crowds 等。综上,算法的系统总时延小于 Crowds 等。

4 结论

根据移动互联网的新特点,针对现有匿名算法面向静态的网络拓扑结构,负载代价较高等不足,提出了适合移动互联网的源地址动态变化匿名算法,实现了发送方匿名。该算法动态隐藏源地址,能适应动态变化的拓扑结构;匿名度较高,能在开放的链路上提供匿名服务;链路长度短,带宽代价小,无需分发密钥,加解密次数少,特别适合移动互联网有限的带宽和计算资源;时延时间短,可用于无连接的网络服务,也可提高匿名通信的实时性。因此,非常适合移动互联网的结构特点及匿名服务需求。算法也可用于有线网络,妥善处理了移动互联网络接入有线互联网后的兼容问题。本文算法路由采用网段自有的路由协议具备较强的可移植性。但是,也正因为如此,匿名性能在一定程度上依赖于网络使用的路由协议,在以后的研究工作中,将会对移动互联网络的路由协议进行研究,将匿名算法和移动互联网路由协议相结合,寻找适合移动互联网的匿名路由协议。另外,研究算法在位置隐私保护中的应用,研究适合移动互联网络用户的位置隐私保护方案。

参考文献:

[1] 张宏科.移动互联网的现状与未来[J].电信科学,2004,10:5-8.

[2] Security Challenges in the future mobile Internet[EB/OL].(2002). http://www.pampas.eu.org/Position_Papers/NEC.pdf.

[3] Pfitzmann A,Waidner M.Networks without user observability[J]. Computers & Security,1987,6(2):158-166.

[4] Waidner M.Unconditional sender and recipient untraceability in spite of active attacks[C]//LNCS 434:Eurocrypt'89.Berlin:Springer Verlag,1989:302-319.

[5] Chaum D.The dining cryptographers problem:Unconditional sender and recipient untraceability[J].Journal of Cryptology,1988,1(1):65-75.

[6] The Free Haven Project.Anonymizer.com[EB/OL].(2004-12-01). http://www.freehaven.net/related-comm.html#anonymizer.

[7] Gabber E,Gibbons P B,Matias Y,et al.How to make personalized Web browing simple,secure,and anonymous[C]//LNCS 1318:Proceedings of Financial Cryptography'97.[S.l.]:Springer-Verlag,1997:17-31.

[8] Gruteser M,Grunwald D.Anonymous usage of location-based services through spatial and temporal cloaking[C]//Proceedings of First International Conference on Mobile Systems,Applications,and Services (MobiSys 2003),2003.

[9] Kalnis P,Ghinita G,Mouratidis K.Preserving anonymity in location based aervices,TRB6/06[R].2006.

[10] Reiter K,Rubin D.Crowds:Anonymity for Web transactions[J]. ACM Transactions on Information and System Security,1998,1(1):66-92.

[11] Reed M G,Syverson P F,Goldschlag D M.Anonymous connections and onion routing[J].IEEE Journal on Selected Areas in Communications,1998,16(4):482-494.

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

[13] Jiang S,Vaidya N H,Zhao W.A dynamic mix method for wireless ad hoc networks[C]//IEEE Military Communications Conference (Milcom'01),2001:873-877.

(下转 208 页)