计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2014.20120948
51(10):2318-2328,2014

# 移动对等环境下基于网络编码的隐私保护方案

李致远[1] 毕俊蕾[2] 王汝传[3]
[1](江苏大学计算机科学与通信工程学院 江苏镇江 212013)
[2](江苏大学信息化中心 江苏镇江 212013)
[3](宽带无线通信与传感网技术教育部重点实验室(南京邮电大学) 南京 210003)
(lizhiyuan81@126.com)

# Network Coding-Based Privacy Protection Scheme for Mobile P2P Networks

Li Zhiyuan[1], Bi Junlei[2], and Wang Ruchuan[3]
[1](*School of Computer Science and Telecommunication Engineering, Jiangsu University, Zhenjiang, Jiangsu* 212013)
[2](*Information Center, Jiangsu University, Zhenjiang, Jiangsu* 212013)
[3](*Key Laboratory of Broadband Wireless Communication and Sensor Network Technology (Nanjing University of Posts and Telecommunications), Ministry of Education, Nanjing* 210003)

**Abstract** With the rapid development of mobile peer to peer (MP2P) applications, user privacy requirements have become increasingly urgent. However, in distributed, frequent mobility and decentralized MP2P environments, the existing schemes have various security vulnerabilities. To protect user privacy in MP2P environments, a mutual anonymity node privacy protection scheme (NMA) based on network coding is proposed. Our contributions are described as below. We first design a network coding scheme which can defend against various omniscient adversary attacks. Then, the network coding is used in the MP2P file-sharing application, including the resource searching, the resource requesting, the resource responding and the file download, to protect user's identity, user's location and routing information. The advantages of the scheme lie in the fact that the network coding and mutli-agent can improve the network load balance, the successful rate of information transmission and the anonymity degree. Both theoretical analysis and the experimental results demonstrate that when the percentage of malicious peers is lower than 50%, the NMA scheme not only can protect the efficient information transmission, but also can hide the user's identity and other privacy information.

**Key words** mobile Internet; mobile peer to peer technology; user privacy; mutual anonymity; linear network coding

**摘 要** 随着移动对等应用的快速发展,用户对自身隐私的需求变得越来越迫切.然而,由于在移动对等环境去中心化、拓扑变化性强的特点使得现有方案存在较多安全隐患.鉴于此,提出基于网络编码的节点隐私保护方案.主要工作包括:设计能够抵御万能敌手攻击的网络编码方案;将网络编码应用于移动对等资源共享,包括资源搜索、资源请求、应答及文件下载,实现了用户身份、用户位置及路由信息的隐私保护.方案的优势在于利用网络编码和多代理机制改善了网络的负载均衡、提高了信息传输成功率并

**收稿日期**:2012-10-23;**修回日期**:2013-01-04
**基金项目**:国家自然科学基金项目(61202474,61272074,61201160,61170065);国家"八六三"高技术研究发展计划基金项目(2006AA01Z439,2007AA01Z404);江苏省自然科学基金项目(BK20130528);江苏大学高级专业人才科研启动基金项目(12JDG049)

增强了节点的隐私性.理论分析和仿真实验结果均表明,方案在网络中恶意节点比例低于50%的情况下,不仅可以保障信息的高效传输,同时可以隐藏用户的身份及其他隐私信息.

**关键词** 移动互联网;移动对等技术;用户隐私;互匿名;线性网络编码

**中图法分类号** TP393.08; TP309

随着宽带无线接入技术和智能终端技术的飞速发展,人们获取 Internet 信息和服务的方式发生了深刻的变化,移动对等(mobile peer to peer, MP2P)技术成为近年来移动互联网研究中的一大热点.在基于智能终端(智能手机和平板电脑)的大量 MP2P 应用中,节点的隐私需求变得越来越迫切,其中包括静态的隐私数据保护[1]和动态的节点行为隐私保护.本文针对节点的行为隐私保护进行研究,主要包含节点身份、位置及路由信息的隐私保护.匿名和加密是该类隐私保护技术研究的 2 种主流方案.加密方案的隐私度最高,但是其服务效率偏低;匿名方案比加密方案隐私度要低,但其服务效率却明显提高.考虑到 MP2P 网络环境的动态性、去中心化及资源受限,匿名方案更容易实现 MP2P 资源共享应用的隐私保护.

针对不同的应用场景,当前的匿名隐私保护方案可分为假数据、时空匿名和互匿名 3 类;针对隐私保护的系统结构、隐私保护方案可分为中心服务结构、主从分布式结构和移动点对点结构.假数据[2]和时空匿名模型[3-4]主要是针对位置隐私保护而提出的,并不能实现查询内容和路由信息的隐私保护,因此,它们并不能保障 MP2P 资源共享应用的匿名性.鉴于此,本文主要对互匿名方案进行研究.互匿名不仅可以实现发起者匿名、响应者匿名,还可以实现发起者和响应者的通信匿名.按照匿名过程中消息的转发模式,将现有方法分为 3 种[5]:基于单一消息的转发模式、基于复制消息的转发模式和基于信息分割的转发模式.单一消息的转发模式缺点在于高度动态的 MP2P 环境中,不能保障预先建立路径上的每一个节点都是活跃的.此外,每跳通信间的加解密运算开销较高.对于复制消息的转发模式,其缺点在于流量开销巨大严重影响有效的数据传输.基于信息分割的转发模式为解决匿名问题提供了新的研究方向.在这种模式下,节点可以任意指派匿名集,并通过密钥共享分发或随机走方式转发消息.然而,抗攻击性和效率仍是该类方法具有挑战性的问题.

本文提出了基于网络编码的移动对等节点互匿名隐私保护方案(network coding-based mutual anonymity privacy protection scheme for mobile p2p networks, NMA).NMA 协议利用基于网络编码的互匿名技术,实现了移动对等环境下节点的身份、地理位置及路由信息的隐私保护.NMA 协议的优势在于利用网络编码和多代理机制实现了移动对等节点的隐私安全,改善了网络的负载均衡并提高了信息传输的效率.

## 1 相关工作

1) 基于单一转发消息的匿名通信方式

基于单一转发消息的匿名通信[6-8]也称为基于路径的匿名通信方法.Mix 路由[6]和洋葱路由[7]是基于路径的匿名通信方法的理论基础.然而,这种方法存在着许多缺陷:①资源请求节点必须获得足够的中间节点信息才能预先构造匿名路径,这对于 MP2P 网络环境是困难的;②即便构造了匿名路径,该路径也是不可靠的、难以维护;③由于匿名路径上每一对相邻节点都采用了基于非对称密钥的加/解密机制,因此,加解密运算开销非常高.

2) 基于复制转发消息的匿名通信方式

为了更好地解决 MP2P 环境下的匿名问题,文献[9]采用了基于复制转发信息的匿名通信方式.该方式与单一转发消息的通信方式不同的是,网络中的每一条消息都在传递过程中以广播或多播方式进行多次复制转发.这类匿名方法克服了基于单一转发消息的匿名通信方式中匿名通信路径不可靠的缺陷,但由于采用广播或多播技术导致产生了大量的冗余消息.同时,由于每个节点都必须加解密所收到的数据包,其开销相当大.

3) 基于信息分割的匿名通信方式

基于消息分割的匿名通信方式[10-11]为解决互匿名提供了新的研究方向.这种匿名通信方式的特点是通过把一条消息拆分成多块碎片的方法,实现用户身份、路由和数据信息的匿名.然而,上述方案的抗攻击性和方案的效能仍是具有挑战性的难题.

为了能够解决当前互匿名方法中存在的难题,将安全的网络编码[12-13]技术引入到 MP2P 环境中.网络编码被视为一种特殊的加密技术.网络编码的核心理念是允许和鼓励中间节点进行编码.这样,发起者首先采用网络编码把消息拆分成多块数据碎片,然后把它们以随机游走的机制分发给邻居节点.只有收集到数据碎片的数量高于或等于事先设定阈值的节点才能还原出原始消息内容,而普通节点则无法推断出所收到的消息内容.

## 2 基于网络编码的隐私保护方案

### 2.1 网络编码

发起者将待转发的数据分割成多个由 $k$ 个数据包组成的分组.分组的格式定义为一个二元组的形式,其中的元组分别为组 ID 号和数据段.下面对一个分组的编解码流程进行阐述.

一个数据包的数据段包含来自有限域 $F_q$ 的 $m-k$ 个符号数据,然后,添加 $\varphi\times m$ 个符号数据到分组中作为冗余信息.这样,一个分组就可表示成矩阵 $\boldsymbol{X}$ 的形式,如式(1)所示:

$$\boldsymbol{X}=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1(m-k)} & 1 & 0 & \cdots & 0\\ a_{21} & a_{22} & \cdots & a_{2(m-k)} & 0 & 1 & \cdots & 0\\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots\\ a_{k1} & a_{k2} & \cdots & a_{k(m-k)} & 0 & 0 & \cdots & 1 \end{pmatrix}, \tag{1}$$

式(1)中,$m-k$ 表示数据包的大小;$k$ 表示一个分组中数据包的个数;矩阵 $\boldsymbol{X}$ 的第 $i$ 行表示该分组中的第 $i$ 个数据包;矩阵 $\boldsymbol{X}$ 右侧是 $k\times k$ 的单位矩阵.

考虑到 MP2P 资源共享应用中内容污染的严重性.假设攻击者将 $z$ 个污染包注入 $\boldsymbol{X}$ 中,$z$ 个污染包用矩阵 $\boldsymbol{A}$ 来表示.

1) 源节点编码

从矩阵 $\boldsymbol{X}$ 中计算出分组能够携带的有效信息量为($km-\varphi m-k^2$),冗余列向量可通过式(2)获得:

$$\boldsymbol{RM}=0, \tag{2}$$

其中,$\boldsymbol{R}$ 为冗余矩阵,它是一个 $\varphi m\times km$ 矩阵.$\boldsymbol{R}$ 中的符号数据是从有限域 $F_q$ 上均匀、独立选取的,并且其数值对于中间节点或者攻击者都是公开的.$\boldsymbol{M}$ 是通过对矩阵 $\boldsymbol{X}$ 中的全部列按顺序作堆叠操作得到的.

发起者把矩阵 $\boldsymbol{X}$ 编码成式(3)右侧待传输的 $k$ 个数据包.

$$\begin{pmatrix} e_{11} & e_{12} & \cdots & e_{1m}\\ e_{21} & e_{22} & \cdots & e_{2m}\\ \vdots & \vdots & & \vdots\\ e_{k1} & e_{k2} & \cdots & e_{km} \end{pmatrix}\boldsymbol{X}=\begin{pmatrix} e_{11}\boldsymbol{B}_1+e_{12}\boldsymbol{B}_2+\cdots+e_{1m}\boldsymbol{B}_k\\ e_{21}\boldsymbol{B}_1+e_{22}\boldsymbol{B}_2+\cdots+e_{2m}\boldsymbol{B}_k\\ \vdots\\ e_{k1}\boldsymbol{B}_1+e_{k2}\boldsymbol{B}_2+\cdots+e_{km}\boldsymbol{B}_k \end{pmatrix}, \tag{3}$$

其中,$\boldsymbol{B}_i$ 表示矩阵 $\boldsymbol{X}$ 的第 $i$ 行;$e_{ij}$ 表示 $k$ 个原始数据包的任意线性组合系数.

最后,发起者洪泛这 $k$ 个待传输的数据包给它的邻居节点.

2) 中间节点编码

当编码后的数据包穿越网络时,中间节点对接收到的数据包进行随机的线性组合操作.同时,对其中的单位矩阵进行同样的线性变换.之后向下一跳节点输出相应的编码包.

3) 目的节点解码

分组在网络传输过程中所经历的线性变换可表示成式(4):

$$\boldsymbol{Y}=[\boldsymbol{T}\ \boldsymbol{T}_a]\begin{bmatrix}\boldsymbol{X}\\ \boldsymbol{A}\end{bmatrix}, \tag{4}$$

其中,$\boldsymbol{Y}$ 表示目的节点收到的编码包;$\boldsymbol{T}$ 表示从发起者到目的节点传输过程所经历的线性变换;$\boldsymbol{T}_a$ 表示污染包到达目的节点所经历的线性变换.

目的节点从矩阵 $\boldsymbol{Y}$ 中选择 $k+z$ 个线性独立列,并把它表示为 $\boldsymbol{Y}_i$.矩阵 $\boldsymbol{X}$ 和 $\boldsymbol{A}$ 中与 $\boldsymbol{Y}_i$ 相对应的列分别用 $\boldsymbol{X}_i$ 和 $\boldsymbol{A}_i$ 表示,则式(4)等价于式(5):

$$\boldsymbol{Y}_i=[\boldsymbol{T}\ \boldsymbol{T}_a]\begin{bmatrix}\boldsymbol{X}_i\\ \boldsymbol{A}_i\end{bmatrix}. \tag{5}$$

将 $\boldsymbol{Y}$ 表示成式(6):

$$\boldsymbol{Y}=\boldsymbol{Y}_i\boldsymbol{E}=[\boldsymbol{T}\ \boldsymbol{T}_a]\begin{bmatrix}\boldsymbol{X}_i\boldsymbol{E}\\ \boldsymbol{A}_i\boldsymbol{E}\end{bmatrix}. \tag{6}$$

若$[\boldsymbol{T}\ \boldsymbol{T}_a]$是可逆的,则可得式(7):

$$\boldsymbol{X}=\boldsymbol{X}_i\boldsymbol{E}. \tag{7}$$

这里把矩阵 $\boldsymbol{E}$ 的前 $m-k$ 列表示成 $\boldsymbol{F}$,矩阵 $\boldsymbol{X}$ 表示成 $\boldsymbol{X}=[\boldsymbol{X}_1\quad\boldsymbol{X}_2\quad\boldsymbol{X}_3]$,其中 $\boldsymbol{X}_1$ 相当于矩阵 $\boldsymbol{X}$ 的前 $z$ 列,$\boldsymbol{X}_3$ 相当于矩阵 $\boldsymbol{X}$ 最后的 $k$ 列,$\boldsymbol{X}_2$ 相当于矩阵 $\boldsymbol{X}$ 的剩余列.将式(7)转换成式(8):

$$[\boldsymbol{X}_1\ \boldsymbol{X}_2]=\boldsymbol{\theta G}+\boldsymbol{H}, \tag{8}$$

其中,$\boldsymbol{\theta}$ 表示 $\boldsymbol{X}_i$ 的前 $z$ 列;$\boldsymbol{G}$ 表示 $\boldsymbol{F}$ 的前 $z$ 行和 $\boldsymbol{H}$ 表示 $\boldsymbol{F}$ 最后 $k$ 行.

结合式(2)和式(8)可得式(9):

$$\boldsymbol{B}\begin{bmatrix}\boldsymbol{M}_1\\ \boldsymbol{M}_2\end{bmatrix}=\begin{pmatrix}\boldsymbol{L}\\ -\boldsymbol{R}_2\boldsymbol{P}\end{pmatrix}, \tag{9}$$

其中,$\boldsymbol{R}_2$ 表示 $\boldsymbol{R}$ 最后 $k\times k$ 列,$\boldsymbol{R}_1$ 表示 $\boldsymbol{R}$ 的剩余部

分.向量 $\boldsymbol{M}_1$ 是按矩阵 $\boldsymbol{X}_1$ 中的列顺序堆叠得到的,向量 $\boldsymbol{M}_2$ 是按矩阵 $\boldsymbol{X}_2$ 中的列顺序堆叠得到的,向量 $\boldsymbol{L}$ 是按矩阵 $\boldsymbol{H}$ 中的列顺序堆叠得到的,向量 $\boldsymbol{P}$ 是按矩阵 $\boldsymbol{I}$ 中的列顺序堆叠得到的,而矩阵 $\boldsymbol{B}$ 见式(10):

$$\boldsymbol{B}=\left[\begin{array}{cccc|c} (1-e'_{1,1})\boldsymbol{I} & -e'_{2,1}\boldsymbol{I} & \cdots & -e'_{z,1}\boldsymbol{I} & \\ \vdots & \vdots & & \vdots & \boldsymbol{0} \\ -e'_{1,z}\boldsymbol{I} & -e'_{2,z}\boldsymbol{I} & \cdots & (1-e'_{z,z})\boldsymbol{I} & \\ \hline -e'_{1,z+1}\boldsymbol{I} & -e'_{2,z+1}\boldsymbol{I} & \cdots & -e'_{z,z+1}\boldsymbol{I} & \\ \vdots & \vdots & & \vdots & \boldsymbol{J} \\ -e'_{1,m-k}\boldsymbol{I} & -e'_{2,m-k}\boldsymbol{I} & \cdots & -e'_{z,m-k}\boldsymbol{I} & \\ \hline \multicolumn{4}{c|}{\boldsymbol{R}_1} & \end{array}\right], \tag{10}$$

其中,$e'_{ij}$ 表示矩阵 $\boldsymbol{G}$ 的第 $i,j$ 项;矩阵 $\boldsymbol{I}$ 为 $k$ 阶单位矩阵;零矩阵 $\boldsymbol{0}$ 有 $zk\times k(m-z-k)$ 维;矩阵 $\boldsymbol{J}$ 为 $k\times(m-z-k)$ 阶单位矩阵.

目的节点最后收到的数据包与发起者和攻击者所发送的数据包是线性相关的.如果目的节点收到关于分组的数据包数量大于或等于 $k+z$,并且矩阵 $\boldsymbol{B}$ 是列满秩的,那么式(9)存在唯一解.

## 2.2 基于网络编码的节点隐私保护方案

### 2.2.1 匿名查询

发起者按以下步骤匿名查询所需的资源 $F$:①发起者对查询消息进行编码;②中间节点对查询消息进行解码;③明文形式的查询消息被洪泛或转发.以图 1 为例对匿名查询的工作流程进行说明.在图 1 中,发起者 $I$ 利用网络编码对原始查询消息进行分割和编码,并将编码后的数据碎片发送给它的邻居节点.这些数据碎片在网络中进行传输,直到一个或多个中间节点 $I_d$ 能够获得足够多的数据碎片以恢复原始的查询消息,这类节点称为代理节点.代理节点 $I_d$ 承担了发起者 $I$ 在网络中的角色,转发还原后的查询消息给它的邻居节点.然后,邻近节点再以随机游走的方式转发这条查询消息给它们的邻居节点,直到消息达到资源节点为止.

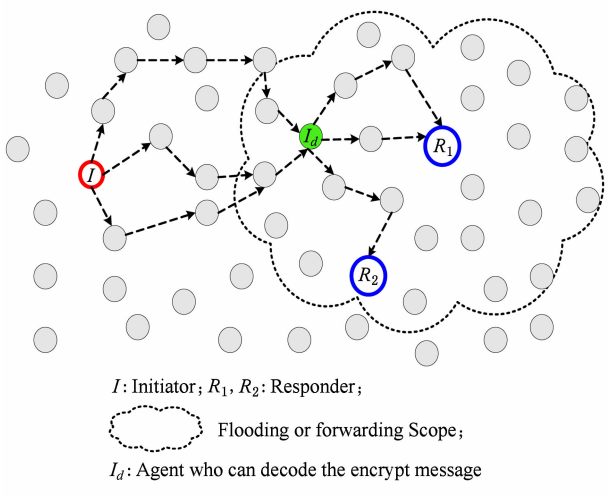



Fig. 1 Anonymous query.

图 1 匿名查询

1) 发起者 $I$ 对查询消息进行编码

发起者 $I$ 利用源节点编码将原始的查询信息分割为由 $k$ 个数据包组成的分组.然后,对分组进行随机线性变换.同时,发起者为每一条查询创建一个序列号 $sq$,$sq$ 是这条查询的 160 b Hash 值,Hash 算法采用 SHA-1 算法.此外,发起者 $I$ 生成 RSA 密钥对.在发送查询消息之前,发起者 $I$ 将公钥 $PK_I$ 嵌入到这些待发送的编码包中.对于每一个编码包,发起者还要附上分组标识号 $bi$ 和包序列号 $sp$.之后,发起者分别发送编码数据包 $\langle e_{ij}X_i, PK_I, sq, bi, sp_i\rangle$,$i=1,2,\cdots,\lceil k/3\rceil$,$j=1,2,\cdots,m$ 给它的邻居节点.之后,这些邻居节点以随机游走方式发送编码信息给它的直接后继.

2) 中间节点 $I_d$ 对查询消息进行解码

当这些编码数据包遍历整个网络时,每个中间节点都要对它们进行随机线性变换.当有中间节点 $I_d$ 能够接收到 $k+z$ 个编码数据包时,该节点就可成功地解码编码数据包,并还原出原始查询信息.

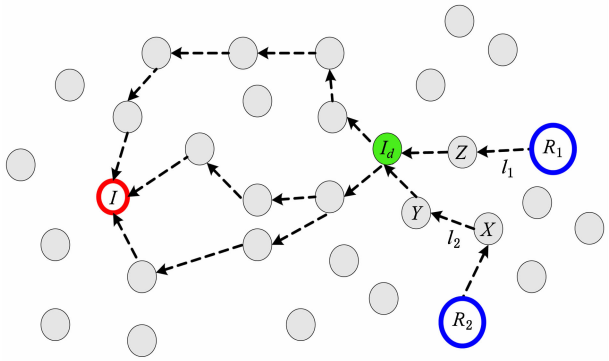
3) 明文形式的查询消息被洪泛或转发

在节点 $I_d$ 恢复出原始的查询信息之后,就直接将该条消息转发给它的邻居节点.消息格式为 $\langle\omega, PK_I, sq\rangle$,其中 $\omega$ 表示原始的查询消息.然后,其邻居节点以随机游走方式转发该条查询消息给它们的后继.当这条查询消息到达一个或多个资源节点时资源发现过程就会终止.

### 2.2.2 匿名响应

当接收节点拥有请求节点所需要的资源时,它就成为一个目的节点 $R$.为了响应该条查询,节点 $R$ 使用 $I$ 的公钥 $PK_I$ 对应答消息进行加密,应答消息包含节点标识符的 Hash 值、$PK_{R_i}$、文件名、文件大小和元数据(作者、出版者、发行日期等).图 2 为匿名响应的示意图.其中,节点 $R$ 以洋葱路由的方式匿名转发应答消息给节点 $I_d$.然后,节点 $I_d$ 利用网络编码对应答消息进行分割和加密,并沿到发起者相反的方向发送这些数据碎片.

为应答发起者 $I$,节点 $R$ 需要提前建立到节点 $I_d$ 的若干条匿名路径.如图 2 所示,$l_1$ 和 $l_2$ 分别为 2 条到节点 $I_d$ 的匿名路径,见式(11)和式(12):




$I$: Initiator; $R_1$, $R_2$: Responder; $l_1$, $l_2$: Anonymous path;
$I_d$: Agent who can decode the encrypt message

Fig. 2 Query reply.

图 2 匿名响应

$$l_1=\{Z,\{I_d,\{\chi_1,sq\}PK_{I_d}\}PK_Z\}, \quad (11)$$

$$l_2=\{X,\{Y,\{I_d,\{\chi_2,sq\}PK_{I_d}\}PK_Y\}PK_X\}, \quad (12)$$

其中 $\chi_i$ 表示被加密的应答消息.

当被加密的应答消息到达节点 $I_d$ 时,$I_d$ 首先对密文进行解密得到 $\chi_i$ 和 $sq$. 然后,$I_d$ 采用线性网络编码对消息 $\chi_i$ 进行分割并编码,并在其本地缓存表中查询 $sq$. 之后,$I_d$ 根据 $sq$ 沿相反的路径转发这些被加密的数据包. 当中间节点收到被加密的碎片包时,它们也会在本地缓存表中查询 $sq$. 如果表中有一条记录和 $sq$ 相匹配,中间节点就会转发被加密的数据包给该条记录中所指向的上游节点. 反之,则会丢弃该数据包. 此外,如果路径上的某些中间节点突然失效,下游的节点则会基于 $sq$ 来重新选择新的后继节点,从而避免单点故障. 当发起者 $I$ 接收到 $k+z$ 个编码数据包时,节点 $I$ 就可成功地对编码数据包进行解码,从而得到被加密的应答信息. 最后,节点 $I$ 使用它的私钥解密被加密的应答消息,从而获得从目的节点发出的明文表示的应答消息.

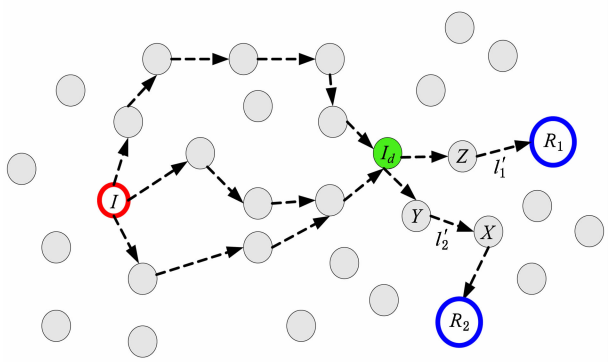
2.2.3 匿名文件传输

在这个阶段,节点 $I$ 首先发送下载请求消息给 $R_i$,然后,节点 $R_i$ 传输目标文件 $F$ 给节点 $I$. 详情描述如下.

1) 文件下载请求

节点 $I$ 从返回的资源列表中选择一个节点作为目标节点 $R$. 然后,节点 $I$ 使用节点 $R$ 的公钥 $PK_R$ 对下载请求消息进行加密. 下载请求消息包含消息类型、文件名和文件格式 3 项. 之后,节点 $I$ 利用线性网络编码方案将下载请求消息分成由 $k$ 个数据包组成的分组并将其进行编码. 最后,节点 $I$ 把 $sq$ 插入到被编码数据包的包头,将它们发送出去.

中间节点根据缓存表中的 $sq$ 将这些数据包转发给节点 $I_d$. 当节点 $I_d$ 搜集到至少 $k+z$ 个编码数据包时,就可成功地恢复出明文显示的下载请求信息. 之后,节点 $I_d$ 预先建立了 2 条到达节点 $R_i$ 的匿名路径 $l_1'$ 和 $l_2'$,如图 3 所示:




$I$: Initiator; $R_1$, $R_2$: Responder; $l_1'$, $l_2'$: Anonymous path;
$I_d$: Agent who can decode the encrypt message

Fig. 3 Download requesting.

图 3 匿名资源下载请求

匿名路径 $l_1'$ 是到达节点 $R_1$ 的路径,见式(13);匿名路径 $l_2'$ 是到达节点 $R_2$ 的路径,见式(14)所示.

$$l_1'=\{Z,\{R_1,\{d_r\}PK_{R_1}\}PK_Z\}, \quad (13)$$

$$l_2'=\{Y,\{X,\{R_2,\{d_r\}PK_{R_2}\}PK_X\}PK_Y\}, \quad (14)$$

其中,$d_r$ 表示下载请求消息.

这条下载请求消息通过路径 $l_1'$ 或路径 $l_2'$ 转发到相应的资源节点 $R_1$ 或者 $R_2$. 如果节点 $R_i$ 可以使用它的私钥 $SK_{R_i}$ 解密该条消息,它将会首先检查消息的类型. 如果消息类型是下载请求报文,它就会为发起者 $I$ 提供文件资源. 否则,将丢弃该报文.

2) 匿名文件传输

目的节点 $R_2$ 利用网络编码来分割和加密文件分片. 然后,节点 $R_2$ 根据缓存表中的 $sq$ 项,将编码后的数据分片沿相反的路径转发到发起者 $I$,如图 4 所示. 在该过程中,关于发起者和目标节点的身份和敏感信息被完全隐藏,详细内容描述如下.

① 文件拆分

文件首先被从逻辑上分割成 $n$ 个片,每一片的大小是 256 KB. 然后,可以得到一张记录所有分片 Hash 值的 Hash 表. 这张 Hash 表是用来检验这些数据块的机密性和完整性. Hash 表的大小为 $160n$ (单位 b). 之后,将 Hash 表和所有的数据块进行编码. 最后,将查询序号 $sq$ 插入到被编码数据包的头部.

② 文件传输

目的节点 $R_2$ 相继将 Hash 表和所有数据分片

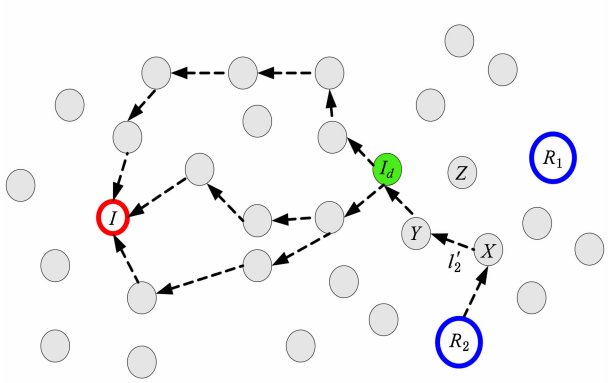



Fig. 4 Anonymous file delivery.

图 4 匿名文件传输

发送到网络上.这些被编码的数据包首先沿着路径 $l_2'$ 到达节点 $I_d$.然后,节点 $I_d$ 根据本地缓存表中的 $sq$ 项转发这些数据包给其邻居节点.之后,邻居节点会执行同样的过程,直到数据包到达发起者 $I$.

③ 文件重构

当发起者 $I$ 收到至少 $\lambda(k+z)$ 个关于 Hash 表的数据包时,节点 $I$ 就可以恢复出原始的 Hash 表,这里的 $\lambda$ 表示文件被分割成 $\lambda$ 个分组.另外,当发起者 $I$ 收到至少 $(k+z)$ 个关于数据分片的数据包时,它就可以恢复出该分片.然后,将该分片的 Hash 值与 Hash 表中相应位置上的 Hash 值进行比较.如果 2 个散列值是相等的,就表明所传输的数据分片是正确的.否则,就会要求资源节点 $R_1$ 或者 $R_2$ 再次重传错误的数据分片.剩余的 $(n-1)$ 个文件分片也都按照上述方法被成功还原和验证.最后,发起者 $I$ 将这些文件分片组合得到所请求的原始文件资源.

## 3 方案的安全性分析

### 3.1 节点的隐私度分析

本节分析 NMA 协议在不同场景下的隐私度.隐私度用匿名度(anonymity degree, AD)的概念来度量,匿名度定义为不能正确地猜测出参与者(发起者和响应者)身份的概率.匿名度越高表明匿名协议的匿名性越好.

1) 发起者(目的节点)随机猜测目的节点(发起者)的身份概率是 $1/(N-1)$,其中,$N$ 表示 MP2P 网络中节点的数量.从外部攻击者的角度看,发起者或目的节点的 AD 是 $(N-2)/(N-1)$.

2) 节点 $I_d$ 实际上是发起者的代理,且每次查询所采用的节点 $I_d$ 是不同的.假设节点 $I_d$ 是网络中唯一的攻击者.节点 $I_d$ 和节点 $R_i$ 之间使用洋葱路由进行通信.如果目的节点 $R_i$ 不是 $I_d$ 的邻居节点,则它的身份会被洋葱路由所隐藏.在这种情况下,目的节点 $R_i$ 的身份将在 $O((N/c)^2)$ 轮被发现[14],其中 $c$ 表示攻击者的数量,显然,这里 $c=1$.因此,目的节点 $R_i$ 的身份将在 $O(N^2)$ 轮被发现.由于 $O(N^2)$ 的数量级非常大,所以目的节点的 AD 可以被视为无穷大.而节点 $I_d$ 和节点 $I$ 之间的消息转发采用随机游走的方式.如果发起者不是节点 $I_d$ 的邻居,那么,发起者的身份被发现的概率是 $1/(N-N_{I_d})$,其中 $N_{I_d}$ 表示节点 $I_d$ 的邻居节点.从内部攻击者 $I_d$ 的角度看,发起者的 AD 是 $(N-N_{I_d}-1)/(N-N_{I_d})$.

3) 下面对共谋攻击下发起者和目的节点的 AD 进行分析.

首先对查询过程中发起者的匿名进行分析.

定义 $x$ 为离发起者最近的恶意节点,$p_d(i)$ 为发起者和第 1 个恶意节点 $x$ 之间存在 $k$ 个节点的概率,$M$ 为恶意节点的数量,$l$ 为发起者和从恶意节点 $x$ 接收编码数据包的代理节点之间的路径长度,$S$ 为接收来自发起者的编码数据包的节点集合.

$H_k(k\geqslant 1)$ 表示通信路径上的第 1 个恶意节点 $x$ 占据路径上第 $k$ 个位置的事件.此时,发起者自身占据了第 0 个位置,且 $H_{k+}=H_k \vee H_{k+1} \vee H_{k+2}\cdots$.令 $I$ 表示发起者处于恶意节点 $x$ 之前的位置上的事件.然后,计算概率 $P(I|H_{1+})$,即攻击者可以正确地猜测出发起者身份的概率.最后,可以得到概率 $P(\overline{I|H_{1+}})$,即发起者的 AD.

$H_k(k\geqslant 1)$ 事件发生的概率见式(15):

$$P_r[H_k]=\left(\frac{N-M}{N}\right)^{k-1}\times\frac{M}{N}. \tag{15}$$

同时,令 $p_e(\omega)$ 表示共谋恶意节点收到 $\omega$,$\omega\geqslant k+z$ 个编码数据包的概率,并令 $p_f$ 表示一个节点愿意帮助转发所收到的数据包的概率,则可得到攻击者正确地猜测出发起者身份的概率 $P(\overline{I|H_{1+}})$,见式(16):

$$P(I\mid H_{1+})=\sum_{k=1}^{l}\left(\frac{N-M}{N}\right)^{k-1}\times \frac{M}{N}\times p_f^{k-1}\times p_d(k)\times p_e(\omega)\leqslant \left(1-\left(1-\frac{M}{N}\right)^{l+1}\right)\times\left(\frac{|S|}{N-1}\right)^{\omega}. \tag{16}$$

最终,得到发起者的 AD,见式(17):

$$P(\overline{I|H_{1+}})=1-P(I|H_{1+})\geqslant$$
$$1-\left(1-\left(1-\frac{M}{N}\right)^{l+1}\right)\times\left(\frac{|S|}{N-1}\right)^{\omega}. \quad (17)$$

采用与上述发起者的匿名度相似的分析方法,对文件传输过程中目的节点的匿名度进行分析,得到目的节点的 AD,见式(18):

$$P(\overline{R|H_{1+}})=1-P(R|H_{1+})\geqslant$$
$$1-\left(1-\left(1-\frac{M}{N}\right)^{l'+1}\right)\times\left(\frac{|F_p|}{N-1}\right)^{\omega}, \quad (18)$$

其中,$l'$表示收到来自恶意节点 $x'$的编码文件分片的代理节点和目的节点之间的路径长度;$F_p$ 表示网络中从目的节点获得文件分片的节点集合.

### 3.2 安全性分析

1) 共谋攻击

共谋攻击是指为了尽可能地确定发起者的身份,相邻近的恶意节点相互协作监管流经它们自身的网络流量,并把自身采集到的流量信息进行分享.对于每一次查询,仅当相邻的恶意节点通过协作的方式获得至少 $k+z$ 个编码数据包时,它们才能够正确地猜测出发起者.由于 NMA 协议中消息的转发采用了随机走的方式,因此,这些恶意节点想收集到至少 $k+z$ 个编码数据包是很困难的,除非网络中恶意节点所占的比例非常大.从直观上看,NMA 协议是非常安全的.式(17)和式(18)分别为网络中存在恶意攻击的情况下发起者和响应者的匿名度计算公式.从理论上分析,NMA 协议也是非常安全的.

2) 时间攻击

时序攻击的定义为恶意节点根据数据包的时间戳去推断本次连接两端的节点身份.例如,利用查询的往返时延(round-trip time, RTT)或者查询的时间差去定位一条传输,并预测出发起者或目的节点的身份.这种攻击对基于路径的互匿名协议或物理网络上的通信协议是非常有效的.然而,NMA 协议运行在逻辑覆盖网络上,且 NMA 协议中的消息转发采用了随机走的方式,这样 RTT 测量根本无法发现发起者和目的节点的真实位置信息,也就无法获得它们的真实身份.因此,NMA 协议可以抵御时间攻击.

3) 前驱节点攻击

前驱节点攻击的主要特点是在匿名通信过程中,发起者需要反复与一个特定的目的节点进行通信.这样,若攻击者俘获了 MP2P 系统中的一些节点,将这些节点组成僵尸网络.那么,这些妥协的节点就只能被动地接收攻击者的指令,比如记录发起者和响应者之间可能的通信.而在 NMA 协议中,解码后的数据包以随机走的方式通过代理节点 $I_d$ 到达目的节点.节点 $I_d$ 好比是前驱节点攻击中"特定的目的节点",敌手自然想要通过它来确定发起者和目的节点的身份及位置信息.但处于发起者和目的节点之间的代理节点 $I_d$ 是不可预测,它是随机地分布在 MP2P 网络上的.因此,敌手想要通过代理节点 $I_d$ 来确定发起者和目的节点的身份是很困难的.即便代理节点被敌手所控制,NMA 协议使得发起者和响应者的匿名度仍然非常高,可以说,在有限的时间内发现发起者和目的节点的身份及其位置信息是不可能的.

4) 追溯攻击

追溯攻击的特点是敌手通过大量被俘获的节点跟踪从目的节点返回的具有相同 $sq$ 数据流的流向.如果具有相同 $sq$ 的数据流的流向同时指向同一个节点,则敌手可以确认该节点即是发起者.这种攻击方法的缺点是它无法得到目的节点的身份和位置信息.而在 NMA 协议中,发起者和代理节点 $I_d$ 之间的路由是随机建立的,这主要是因为节点 $I_d$ 不可预知的.因此,除非敌手控制了网络中的大多数节点,否则,在 NMA 协议中发起者的身份和位置信息也始终是个秘密.

## 4 性能评估

### 4.1 性能评估指标

NMA 协议的性能评估指标包括响应时间、交易成功率、流量开销和匿名的风险性分析.

1) 响应时间

响应时间参数是用户十分关心的性能指标.响应时间定义为从查询发起到发起者收到第 1 个查询响应所需要的时间.

2) 交易成功率

交易成功率是成功完成交易的比例.这里的交易是指文件下载的全过程,包括发起查询、查询响应、发起下载请求和文件分片传输.

3) 流量开销

流量开销是网络管理员所关注的重要指标之一.在实验中,流量开销的定义为隐私通信所招致的额外信令开销,见式(19)所示:

$$msg=(T_{\text{overall}}-T_{\text{downlaod}})/pl, \quad (19)$$

其中,$T_{overall}$表示仿真时间内所产生的总的网络流量;$T_{download}$表示所下载文件的大小和 $pl$ 表示数据包的大小.

为了更加直观,这里采用 NMA 协议和正常 P2P 文件下载所产生的流量开销比作为流量开销实验的仿真指标.

4) 匿名的风险性分析

匿名风险性分析的定义为恶意节点比例不断增加对发起者或目的节点的匿名度的影响.

### 4.2 实验方法

为了评估 NMA 协议的性能,实验采用基于轨迹驱动的模拟方法.移动自组织网 MANET 的拓扑结构是通过基于社交的移动模型(community based mobility model, CMM)[15]产生的.CMM 是一个无线网络拓扑生成工具,它能够模拟移动自组织网络环境中移动场景和社交网络的特征.在本节的仿真实验中,设网络中包含 10 000 个移动节点,并将这些节点部署在 $80\times55\ km^2$ 的区域中.这些节点的初始化位置由 CMM 生成,并且这些节点自组织成 MANET 结构.然后,在 MANET 上建立一个移动覆盖网络拓扑结构,网络拓扑的数据来源于 DSS Clip2 的日志数据,该日志数据时间为 2000-12—2001-06,这些数据是从 dss.clip2.com 网站上下载的.所下载的数据集包含节点的 ID 号、IP 地址、主机名、端口号、ping 的时间、速度等.

假设实验的仿真场景是 MP2P 文件共享应用.仿真实验参数如表 1 所示,所有的实验参数都写在.conf 的配置文件中.

**Table 1 Simulation Parameters**

**表 1 仿真实验参数**

| Parameters | Default Value | Description |
|---|---|---|
| MAC | 802.11 | Media access control |
| $R_{tr}$/m | 250 | Transmission distance |
| $B_w$/Mbps | 11 | Bandwidth |
| BER/% | 10 | Bit error rate |
| Mobility Model | Random Waypoint | Mobility model |
| Speed/(m·s$^{-1}$) | 1.4 | Moving speed of nodes |
| Packet Size/b | 256 | Packet size |
| $\gamma$/% | 10 | The initial percentage of collaborating malicious peers |
| Simulation Time/s | 3 600 | Simulation time |

通过为节点分配以秒为单位的生命周期来模拟节点的动态变化.节点的生命周期平均值被设置为 600 s,且节点的生命周期随着时间的增加而递减.当节点的生命周期递减到零时,该节点就会离开 MP2P 网络.同时,随机地选择新的节点进入 MP2P 网络.

最后,依据性能评估指标,将 NMA 协议分别与 NQ(normal query)、P2P-SC(peer-to-peer spatial cloaking algorithm)[3]算法、CDAShip(clinical document architecture secure health information protocol)协议[10]进行了对比.

### 4.3 实验结果与分析

本实验以不施加隐私保护的查询方案为基准进行对比分析.图 5 描述了 NQ,NMA,CDAShip 协议和 P2P-SC 算法的响应时间的累积分布曲线.响应时间的累积分布曲线是用来表征上述协议和算法的响应时间的收敛状况.其中,NMA 协议的响应时间的收敛速度比 P2P-SC 算法快 2 倍、比 CDAShip 协议快 1 倍左右,与不具备匿名功能的查询算法 NQ 相比,NMA 协议的收敛速度是其的 4/5.该实验结果表明,NMA 协议采用编解码来实现隐私保护牺牲了约 30%的时间开销.表明该方案更适合实时性较弱的资源共享方案,如文件共享.对于另外两项实验的结果是和 P2P-SC 算法与 CDAShip 协议的实现机制分不开的.P2P-SC 算法采用 $k$-匿名模型来实现时空的匿名,这种方法尽管可以保障发起者的匿名隐私,但却未明确指出查询信息的返回路径,这使得查询的响应时间大大增加;CDAShip 协议利用 Shamir 的密钥共享方案(secret sharing scheme, SSS)[16]实现了内容的隐私保护,这种方案的隐私度较高,但是需要同时获得多个密钥携带者的信息才

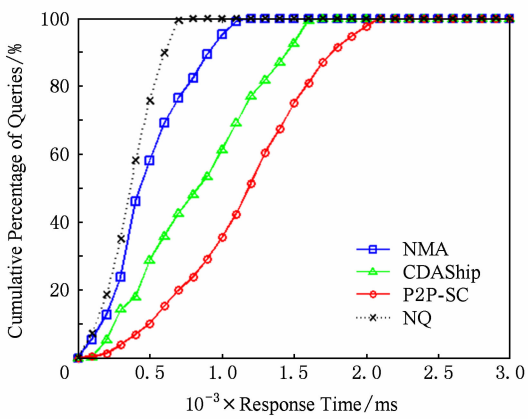



Fig. 5 Cumulative distribution of response time.

图 5 响应时间的累积分布曲线

能解码出正确的内容,类似多方计算的思想.由于MP2P环境的动态性和复杂性使得解码速度变慢,响应时间增长.

图6描述了非匿名查询NQ和3种匿名协议的响应时间的可扩展性.显然,为了实现匿名通信并保护用户的行为隐私安全,3种方案都导致了更多的开销,其中实现隐私保护的方案越复杂,开销也就越大,可扩展性也就越差.从图6不难发现,NMA协议更接近非匿名查询NQ的响应时间,其差异性随着网络规模的增大有减小的趋势,这表明基于网络编码的NMA方案更适用于移动P2P网络环境.NMA方案与其他2种匿名方案相比的实验结果是,在网络规模少于3 000个节点时,它们的响应时间几乎是相同的.当网络规模大于3 000个节点时,它们的响应时间的差距变得越来越大.其原因在于NMA协议响应时间的可扩展性主要与网络上的文件资源分布(该分布服从Zipf定律)有关系,而与网络规模没有直接的联系.编解码所产生的开销对该实验环境下的响应时间影响较弱.因此,NMA协议响应时间的可扩展性较之其他2类匿名隐私保护方法更强.

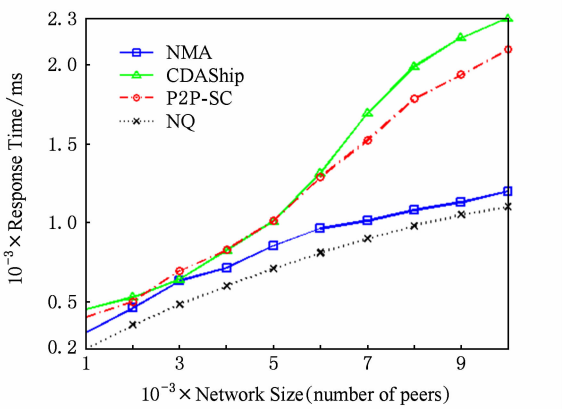



Fig. 6 Scalability of NMA.

图6 NMA的可扩展性

图7描述了网络中恶意节点比例不断变化下交易成功率仿真.在本次实验中,假设恶意节点可以发起各种恶意攻击,包括监听、伪造、丢弃各类流经它们的数据包等.图7显示,网络中恶意节点比例低于40%左右时,NMA协议的交易成功率要高于其他协议;当网络中恶意节点数目高于50%时,NMA协议的交易成功率低于P2P-SC算法,却仍高于CDAShip协议.图7中的实验结果还表明网络中恶意节点的比例低于50%时,NMA协议的可靠性更高且其交易成功率可达到88%以上.然而,随着网络中恶意节点比例的增加,NMA协议的性能迅速下降.原因在于尽管NMA协议利用了安全的弹性网络编码,使得它具有较强的抵御监听和共谋攻击的能力.然而,当大多数的中间恶意节点选择伪造、中断和搭便车攻击时,善意的节点无法收到至少$k+\varepsilon$个编码数据包,能够正确地恢复出原始信息的能力自然就大大降低.最后,NMA交易的成功率迅速下降.而P2P-SC算法没有采用多方计算的策略,因此它不会明显遭受到伪造和丢包之类的主被动攻击的影响.这种情况下,P2P-SC算法的交易成功率较高.

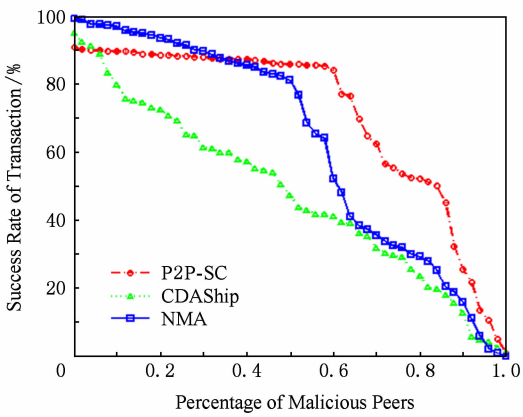



Fig. 7 Percentages of malicious peers versus success rate.

图7 恶意节点比例变化下的交易成功率仿真

图8描述了3种匿名协议和算法的匿名通信带来的额外流量开销.图8显示,CDAShip协议和P2P-SC算法随着搜索范围的增加呈线性增长,未见收敛的趋势.对于NMA协议,当搜索范围小于1 000时,流量开销比从1.05变化到1.2,表明NMA协议导致了5%~20%的额外流量开销.此外,图8还表明,当搜索范围大于1 000时,流量开销比在1.17和1.23之间波动,并最终收敛到1.18附近.这意味着NMA协议所导致的额外流量开销平均应

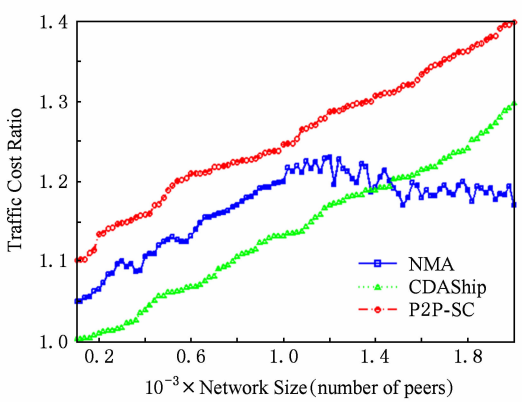



Fig. 8 Traffic cost.

图8 流量开销

为 18%.事实上,NMA 协议所产生的额外流量开销主要取决于发起者和响应者之间的平均路径长度.一般情况下,平均路径长度越长 NMA 协议所产生的额外流量开销就越大.然而,随着 MP2P 覆盖网络规模的增大,网络中任意 2 个节点之间的平均路径长度趋于一个固定值,正如图 8 所反映的趋势,这也使得 NMA 协议所导致的额外流量开销收敛于 18%.为了保证用户的隐私信息,牺牲 18%的额外流量开销对于 MP2P 环境是完全可接受的.

图 9 分析了 3 类协议匿名度的风险性.在图 9 中,横坐标表示网络中恶意节点所占的比例,纵坐标表示 NMA 协议的匿名度,即发起者或者响应者的匿名度.如图 9 所示,当网络中恶意节点的数目较少时,NMA 协议的匿名度几乎可以达到 100%.之后,随着网络中恶意节点所占比例的增加,NMA 协议的匿名度逐渐降低.当网络中恶意节点所占的比例大于 55%时,NMA 协议的匿名度低于 P2P-SC 算法;当网络中恶意节点所占的比例大于 60%时,NMA 协议的匿名度低于 CDAShip 协议.当网络中恶意节点所占的比例超过 90%时,NMA 协议的匿名度几乎降低为零.上述结果表明,网络中恶意节点比例较低的环境对 NMA 协议的匿名度影响不大.当网络中恶意节点所占的比例从 40%增加到 70%时,前驱节点攻击和共谋攻击对 NMA 协议的匿名度影响较大.当网络中恶意节点的比例从 80%增至 100%时,追溯攻击对 NMA 协议的匿名度影响较大.实验结果与方案的安全性分析结果完全一致.综上,NMA 协议的性能和它的匿名度在网络中恶意节点的比例低于 50%时是最优的.在恶意节点的比例高于 50%时,NMA 协议会受到各种网络攻击的影响,其匿名度和性能都会被大大削弱.

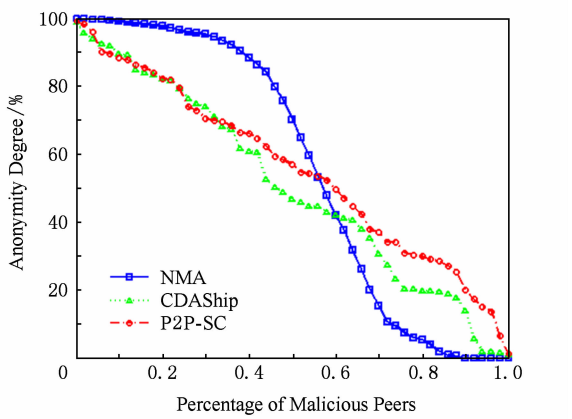



Fig. 9 Risk analysis of anonymity.

图 9 匿名的风险性分析

## 5 结 论

本文提出移动对等环境下基于网络编码的节点隐私保护方案 NMA.本文的主要工作包含 2 个方面:1)设计一种能够抵御各种恶意攻击的网络编码方案;2)基于上述网络编码方案,建立新的互匿名通信协议从而实现节点身份、节点位置及路由信息的隐私保护.然后,从理论上分析了 NMA 协议的隐私度和安全性.最后,从响应时间、通信开销、资源下载成功率和匿名度方面对 NMA 协议进行性能评估.结果显示,当恶意节点所占的比例低于 50%时,NMA 协议的各项性能均优于同类的互匿名通信协议.表明 NMA 协议不仅可以保障正常的 MP2P 应用,同时可以隐藏用户的身份及其他隐私信息.然而,当恶意节点所占的比例高于 60%时,目前包括 NMA 在内的任何互匿名通信协议均不能保障用户的隐私安全.今后的工作是继续研究多方安全计算理论,并尝试性地解决该问题.目标是设计一种更好的用户隐私保护模型,该模型在恶意节点高于 60%时,仍能够有效地保护用户隐私安全.

## 参 考 文 献

[1] Fang Weiwei, Ren Jiang, Xia Hongke. Heterogeneous distributed linear regression privacy-preserving modeling [J]. Journal of Computer Research and Development, 2011, 48(9): 1685-1692 (in Chinese)
(方炜炜,任江,夏红科. 异构分布的多元线性回归隐私保护模型[J]. 计算机研究与发展, 2011, 48(9): 1685-1692)

[2] Yang Q, Alvin L, Ruan X J, et al. Location privacy protection in contention based forwarding for VANETs [C]//Proc of the 53rd IEEE Global Communications Conf. Los Alamitos, CA: IEEE Communications Society, 2010: 1-5

[3] Chow C Y, Mokbel M F, Liu X. Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments [J]. GeoInformatica, 2011, 15(2): 351-380

[4] Huo Zheng, Meng Xiaofeng. A survey of trajectory privacy-preserving techniques [J]. Chinese Journal of Computers, 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)

[5] Xiao R Y. Survey on anonymity in unstructured peer-to-peer systems [J]. Journal of Computer Science and Technology, 2008, 23(4): 660-671

[6] Chaum D. Untraceable electronic return addresses, and digital pseudonyms [J]. Communications of the ACM, 1981, 24 (2): 84-90

[7] Goldschlag D, Reed M, Syverson P. Onion routing [J]. Communications of the ACM, 1999, 42(2): 39-41

[8] Li X, Xu Z, Zhang X. Low-cost and reliable mutual anonymity protocols in peer-to-peer networks [J]. IEEE Trans on Parallel and Distributed Systems, 2003, 14(9): 829-840

[9] Sherwood R, Bhattacharjee B, Srinivasan A. P5: A protocol for scalable anonymous communication [J]. Journal of Computer Security, 2002, 13(6): 839-876

[10] Jens H W J, Christina O. Protecting privacy during peer-to-peer exchange of medical documents [J]. Information Systems Frontiers, 2012, 14(1): 87-104

[11] Liu Y H, Han J S, Wang J. Rumor riding: anonymizing unstructured peer-to-peer systems [J]. IEEE Trans on Parallel and Distributed Systems, 2011, 22(3): 464-475

[12] Jing D, Reza C, Cristina N R. Secure network coding for wireless mesh networks: Threats, challenges, and directions [J]. Computer Communications, 2009, 32(17): 1790-1801

[13] Cai N, Chan T. Theory of secure network coding [J]. Proc of the IEEE, 2011, 99 (3): 421-437

[14] Wright M, Adler M, Levine B N, et al. An analysis of the degradation of anonymous protocols [C] //Proc of the 9th Symp on Network and Distributed System Security. Piscataway, NJ: IEEE, 2002: 1-13

[15] Musolesi M, Mascolo C. Designing mobility models based on social network theory [J]. ACM SIGMOBILE Mobile Computing and Communications Review, 2007, 11(3): 59-70

[16] Shamir A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612-613

**Li Zhiyuan**, born in 1981. Lecturer of Jiangsu University. Member of China Computer Federation and ACM. His main research interests include privacy protection for mobile P2P networks and Internet of things.

**Bi Junlei**, born in 1981. Lecturer of Jiangsu University. Member of China Computer Federation and ACM. Her main research interests include Internet of things and cloud computing.

**Wang Ruchuan**, born in 1943. Professor and PhD supervisor of Nanjing University of Posts and Telecommunications. Senior member of China Computer Federation. His main research interests include P2P computing, the security of network, sensor networks, etc.