软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2016,27(8):1891−1903 [doi: 10.13328/j.cnki.jos.005096]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

隐私保护的信息熵模型及其度量方法*

彭长根[1,2,3], 丁红发[4,5], 朱义杰[2,3], 田有亮[1,2,3], 符祖峰[2]

[1](贵州省公共大数据重点实验室(贵州大学),贵州 贵阳 550025)

[2](贵州大学 计算机科学与技术学院,贵州 贵阳 550025)

[3](贵州大学 密码学与数据安全研究所,贵州 贵阳 550025)

[4](贵州大学 理学院,贵州 贵阳 550025)

[5](贵州财经大学 信息学院,贵州 贵阳 550025)

通讯作者: 彭长根, E-mail: peng_stud@163.com

摘 要: 隐私的量化是隐私保护技术的重要支撑,信息熵作为信息的量化手段,自然可以用于解决隐私度量问题.基于Shannon信息论的通信框架,提出了几种隐私保护信息熵模型,以解决隐私保护系统的相关度量问题,主要包括:隐私保护基本信息熵模型、含敌手攻击的隐私保护信息熵模型、带主观感受的信息熵模型和多隐私信源的隐私保护信息熵模型.在这些模型中,将信息拥有者假设为发送方,隐私谋取者假设为接收方,隐私的泄露渠道假设为通信信道;基于这样的假设,分别引入信息熵、平均互信息量、条件熵及条件互信息等来分别描述隐私保护系统信息源的隐私度量、隐私泄露度量、含背景知识的隐私度量及泄露度量;以此为基础,进一步提出了隐私保护方法的强度和敌手攻击能力的量化测评,为隐私泄露的量化风险评估提供了一种支撑;最后,针对位置隐私保护的应用场景,给出了具体的信息熵模型及隐私保护机制和攻击能力的度量及分析.所提出的模型和隐私量化方法,可以为隐私保护技术和隐私泄露风险分析与评估提供可行的理论基础.

关键词: 隐私保护;通信模型;信息熵;隐私度量;风险评估

中图法分类号: TP309

中文引用格式: 彭长根,丁红发,朱义杰,田有亮,符祖峰.隐私保护的信息熵模型及其度量方法.软件学报,2016,27(8):1891−1903. http://www.jos.org.cn/1000-9825/5096.htm

英文引用格式: Peng CG, Ding HF, Zhu YJ, Tian YL, Fu ZF. Information entropy models and privacy metrics methods for privacy protection. Ruan Jian Xue Bao/Journal of Software, 2016,27(8):1891−1903 (in Chinese). http://www.jos.org.cn/1000-9825/5096.htm

Information Entropy Models and Privacy Metrics Methods for Privacy Protection

PENG Chang-Gen[1,2,3], DING Hong-Fa[4,5], ZHU Yi-Jie[2,3], TIAN You-Liang[1,2,3], FU Zu-Feng[2]

[1](Guizhou Provincial Key Laboratory of Public Big Data (Guizhou University), Guiyang 550025, China)

[2](College of Computer Science and Technology, Guizhou University, Guiyang 550025, China)

[3](Institute of Cryptography & Data Security, Guizhou University, Guiyang 550025, China)

[4](College of Science, Guizhou University, Guiyang 550025, China)

[5](School of Information, Guizhou University of Finance and Economics, Guiyang 550025, China)

* 基金项目: 国家自然科学基金(61262073, 61363068); 全国统计科研重点项目(2013LZ46); 贵州省教育厅创新团队项目(2013-09)

Foundation item: National Natural Science Foundation of China (61262073, 61363068); National Statistics Key Program of China (2013LZ46); Innovation Team Project of Guizhou Provincial Education Department (2013-09)

收稿时间: 2016-01-15; 采用时间: 2016-04-14

Abstract: The quantification of privacy plays an important role in the privacy protection. Information entropy as a quantitative method of information can be used to solve the problem of privacy measurement. In order to realize the privacy metrics, several models of privacy information entropy are proposed based on Shannon's Information Theory. These models include the basic information entropy model of privacy protection, the information entropy model of privacy protection with adversary, the information entropy model of privacy protection with subjective feelings and multi-source information entropy model of privacy protection. In these models, the information owner is assumed to be the sender, privacy attacker is assumed as to be the recipient, and the privacy disclosure course can be regarded as a communication channel. Based on these assumptions, the entropy, mutual information, conditional entropy, and conditional mutual information are introduced to represent measurement of privacy, privacy disclosure, and privacy and disclosure with background knowledge for the privacy protection system. Furthermore, the quantitative evaluation of privacy protection strength and adversary ability is provided to support quantitative risk assessment for privacy disclosure. Finally, the specific information entropy model, measurement and analysis of privacy protection algorithms, and adversary ability are supplied for location privacy protection application. The proposed models and privacy metrics can be used as fundamental theory for the privacy protection technology and privacy disclosure risk assessment.

Key words: privacy protection; communication model; information entropy; privacy metric; risk assessment

隐私保护的研究起步较早,但近年来突然受到产业界和学术界的广泛关注,是因为大数据的不期而至.大数据的迅速发展让学术界始料未及,大数据的理论研究已经落后于产业需求,尤其是隐私保护成为了大数据应用的主要瓶颈,移动网络、社交网络、位置服务等新型应用的推进,使隐私问题更加突出.关于隐私保护目前有两个方向值得关注:一是研究更有效的隐私保护算法;二是研究隐私泄露风险分析与评估,以解决数据的可用性与隐私保护之间的平衡.隐私保护算法目前主要集中在匿名方法,包括 *K*-匿名(*K*-anonymity)、*L*-多样性(*L*-diversity)匿名和 *t*-接近(*t*-close)匿名及其衍生的方法.隐私度量最早起源于相关匿名算法[1].在匿名隐私保护算法的研究中,不时有学者关注隐私量化问题,尤其是在定位服务领域,位置匿名和轨迹匿名算法已有不少涉及隐私度量的初步研究[2,3].然而隐私泄露涉及因素众多,设计有效的隐私保护算法仍然是挑战性问题.但政府及企业数据开放共享中迫切的隐私保护需求,促使我们不得不在可用性与隐私泄露之间寻求一种平衡.要解决这个问题,隐私风险分析及评估不失为一种可行解决方案.但隐私风险分析及评估,尤其是量化隐私风险,势必会涉及隐私度量问题.从这些分析来看,隐私度量的研究具有十分重要的理论意义和应用价值.

信息熵作为信息度量的有效工具,在通信领域已展现出其重要的贡献[4].隐私作为一种信息,自然可以考虑用熵来量化.为此,不少学者或多或少进行了探索,比如事件熵、匿名集合熵、条件熵等[5−7].但其研究还较为零散,更多地是针对某一特定领域,如位置隐私保护,目前还尚未形成统一的模型及体系.其应用范围也受到限制,特别是隐私是具有时空性的,与人的主观感受也有关系,不同的人对同一隐私的认同可能不同.鉴于以上分析,本文旨在参考 Shannon 信息论的通信框架[8],提出几种隐私保护信息熵模型,包括隐私保护基本信息熵模型、含敌手攻击的隐私保护信息熵模型、带主观感受的信息熵模型和多隐私信源的隐私保护信息熵模型.在这些模型中,将信息拥有者假设为发送方,隐私谋取者假设为接收方,隐私的泄露渠道假设为通信信道.基于这样的假设,分别引入隐私信息熵、平均互信息量、条件熵及条件互信息等来分别描述隐私保护系统信息源的隐私度量、隐私泄露度量、含背景知识的隐私度量及泄露度量.以此为基础,进一步提出了隐私保护方法的强度和敌手攻击能力的量化测评,力图为隐私泄露的量化风险评估提供一种理论支持.

本文第 1 节介绍相关工作.第 2 节利用信息熵的通信模型,提出具有通用特性的隐私度量信息熵模型.第 3 节在第 2 节所提出的信息熵模型下提出一种隐私度量方法及评价体系.第 4 节将本文所提出的隐私度量方法及评价体系应用于位置隐私保护,并分析其有效性.第 5 节给出总结.

1 相关工作

Shannon 提出的信息熵理论[8]解决了信息的量化和通信的理论基础.较早将信息熵考虑到隐私度量的研究是 Diaz 等人[5]和 Serjantov 等人[6],他们提出了用信息熵来度量匿名通信系统的匿名性.假定攻击者的目的是要确定消息的发送者(或接收者)的真实身份,系统中每个用户都以一定的概率被猜测为消息的真实发送者或接

收者,将攻击者猜测某用户是真实发送者或接收者看成一个随机变量 X,用信息熵 $H(X)=-\sum p(x)\log p(x)$ 来量化系统的隐私水平.随后,有不少学者将信息熵应用于某些具体领域的隐私度量,如位置服务、社交网络和数据挖掘等领域[2,3,9−21].对于不同的方案,其随机变量的概率表现形式和对熵的处理方式不同.

在位置服务领域,2007 年,Hoh 等人[9,10]提出了基于信息熵的隐私度量方法度量轨迹跟踪的不确定度,其中,随机变量的概率表现为每个位置实例包含在当前跟踪车辆轨迹的概率.2009 年,Ma 等人[11]提出了在 V2X 车联网系统中信息熵的隐私度量方法,其中,随机变量的概率表现为每个位置信息关联到某特定用户的概率.该方法还考虑了随机变量的概率随着时间的变化而更新的情况,即攻击者的累积信息对系统隐私的影响.同年,林欣等人[12]针对 LBS 中的连续查询问题,提出了一种连续查询攻击算法.他们指出,匿名集的势不再适合作为查询该算法匿名性的度量,并提出了基于信息熵的度量方法,其中,随机变量的概率表现为每个用户 u_i 是查询 q 的真正发出者的概率,信息熵计算为 $H(q)$,用 $AD(q)=2^{H(q)}$度量系统的隐私水平.2011 年,Shokri 等人[2]将位置隐私的度量准则分为精确性、确定性和正确性:精确性度量为攻击者猜测事件的置信区间,确定性度量为攻击者猜测的不确定性,正确性度量为攻击者出错的概率.其中,精确性的度量是基于信息熵的度量方法,随机变量的概率表现为每个观测事件是真实事件的概率.2012 年,Chen 等人[13]针对 LBS 查询隐私进行度量,随机变量的概率表现为攻击者在无背景知识和有背景知识两种情况下的判断用户 u_i 是查询 q 的真实发出者的条件概率,并利用互信息 $I(U|q;\langle r,t,q\rangle)=H(U|q)-H(U|\langle r,t,q\rangle)$度量系统的隐私水平.同年,王彩梅等人[3]针对 LBS 中的轨迹隐私保护方法 Silent Cascade 提出了基于信息熵的隐私度量方法,随机变量的概率表现为某用户的每条可能轨迹的概率,特定用户的熵计算为 $H(u_i)$,并用标准熵 $D(u_i)=H(u_i)/H_{\max}(u_i)$度量为系统的隐私水平.2014 年,文献[14,15]均采用了信息熵度量了 LBS 系统的隐私水平.

在社交网络领域,2010 年,Ngoc 等人[16]针对社交网络隐私泄露的情况,提出了基于信息熵的隐私度量方法,以帮助用户判断所发布信息的隐私水平,其随机变量的概率表现为事件 X 的取值 x 的概率.2012 年,Yang 等人[17]总结了社交网络中的风险,并利用信息熵和互信息度量系统的隐私水平.

此外,在其他领域,用信息熵作为隐私度量也有所涉及.文献[18,19]研究了信息熵用于数据挖掘的隐私度量,文献[20]研究了信息熵用于匿名系统的隐私度量,文献[21]研究了信息熵用于增价竞标中竞标人的隐私度量.Wagner 等人[6]对当前存在的隐私度量方法进行了综述,根据度量系统的输出将隐私度量方法分成 8 类,其中不确定度的分类是根据信息熵度量来划分的的.

综上所述,目前存在的基于信息熵进行隐私度量的理论体系较为零散,缺乏统一的模型基础.针对上述问题,本文试图将隐私保护系统看作一个通信传播模型,力图探讨较为通用的隐私度量信息熵模型,解决隐私度量的一些基本概念和基础体系.

2 隐私保护信息熵模型

本文的出发点是将信息拥有者假设为发送方,隐私谋取者(敌手)假设为接收方,隐私的泄露渠道假设为通信信道.

发送方拥有的信息集称为隐私信源,用随机变量 X 表示,X 是由所有的离散基本泄露事件的隐私消息构成的隐私消息空间,即 $\{x_1,x_2,\ldots,x_n\}$,其中,$x_i(i=1,2,\ldots,n)$为基本泄露事件的隐私消息;接收方获取的信息集称为隐私信宿,用随机变量 Y 表示,它是由敌手获取的所有基本隐私消息构成,即 $\{y_1,y_2,\ldots,y_m\}$,其中,$y_j(j=1,2,\ldots,m)$为敌手获取的某个隐私消息.相应地,某一种具体的隐私保护算法可以看作是对隐私消息进行转换、编码的方法,它能够对隐私消息进行干扰,进而实现对隐私信息的保护.其中,隐私保护算法的全体构成隐私保护机制空间称为隐私保护机制源.敌手在一定背景知识下对隐私信息的挖掘与分析手段称为隐私攻击,所有隐私方法的的全体称为隐私攻击空间.

以此假设为基础,本节将基于 Shannon 信息论的通信框架[8]提出几种隐私保护信息熵模型,包括隐私保护基本信息熵模型、含敌手攻击的隐私保护信息熵模型、带主观感受的信息熵模型和多隐私信源的隐私保护信息熵模型.通过引入隐私信息熵、平均互信息量、条件熵及条件互信息等来分别描述隐私保护系统信息源的隐

私度量、隐私泄露度量、含背景知识的隐私度量及泄露度量.

2.1 隐私保护基本信息熵模型

这里,我们首先假设敌手无任何隐私攻击能力,敌手仅通过信道观测到隐私信息,并只考虑离散单隐私信源的情形.模型定义如图 1 所示.

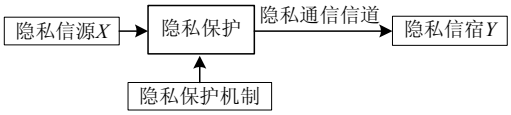


Fig.1 Communication model of privacy protection with single privacy information source

图 1 单隐私信源隐私保护通信模型

设单隐私信源 X 的数学模型可以表示为

$$\begin{pmatrix} X \\ P(X) \end{pmatrix}=\begin{pmatrix} x_1 & x_2 & \dots & x_i & \dots & x_n \\ p(x_1) & p(x_2) & \dots & p(x_i) & \dots & p(x_n) \end{pmatrix} \tag{1}$$

其中,$0\leqslant p(x_i)\leqslant 1$, $\sum_{i=1}^{n} p(x_i)=1$.同理,隐私信宿 Y 的数学模型可表示为

$$\begin{pmatrix} Y \\ P(Y) \end{pmatrix}=\begin{pmatrix} y_1 & y_2 & \dots & y_j & \dots & y_m \\ p(y_1) & p(y_2) & \dots & p(y_j) & \dots & p(y_m) \end{pmatrix} \tag{2}$$

其中,$0\leqslant p(y_j)\leqslant 1$, $\sum_{j=1}^{m} p(y_j)=1$.

针对该模型,定义隐私信源熵 $H(X)$:

$$H(X)=-\sum_{i=1}^{n} p(x_i)\log_2 p(x_i) \tag{3}$$

$H(X)$用于刻画隐私信源的平均隐私信息量,也是隐私信源的隐私不确定程度.$H(X)$越大,隐私泄露可能性就越小,从而它也可以用于衡量隐私的保护程度.在没有外部条件影响时,该值是一个确定的值.

当隐私信宿 Y 在获取一些隐私信息条件下时,关于隐私信源的不确定程度,可以引入隐私条件熵 $H(X/Y)$刻画,其定义为

$$H(X/Y)=-\sum_{j=1}^{m}\sum_{i=1}^{n} p(x_i y_j)\log_2 p(x_i/y_j) \tag{4}$$

该条件熵表示隐私信宿在收到 Y 后,隐私信源 X 仍然存在不确定程度.该不确定程度是隐私泄露信道的干扰(隐私保护)造成的,即敌手在长期观测隐私信源过程中,由于隐私保护机制的保护,敌手对隐私信源仍然存在一定的未知.易证明,这种隐私信息熵满足 Shannon 信源熵的基本性质[4].即具有非负性、对称性、扩展性、确定性、可加性、极值性、上凸性等,并满足极大离散熵定理,在此不再赘述.

下面引入平均隐私互信息量 $I(X;Y)$来刻画信道上隐私泄露程度,定义为

$$I(X;Y)=\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i y_j)\log_2\frac{p(x_i/y_j)}{p(x_i)}. \tag{5}$$

$I(X;Y)$表示了隐私信源 X 和隐私信宿 Y 之间交互的平均信息量,即在信道上传播的隐私信息量.它正好可以刻画隐私的整体泄露程度,从而可以作为隐私的泄露度量.

2.2 含敌手攻击的隐私保护信息熵模型

上一节提出的隐私保护基本信息熵模型,客观上描述了无敌手攻击或敌手无攻击能力情况下的隐私度量问题.在实际系统中,往往存在着隐私攻击分析,敌手可以在一定的背景知识下进行攻击分析,模型定义如图 2 所示.

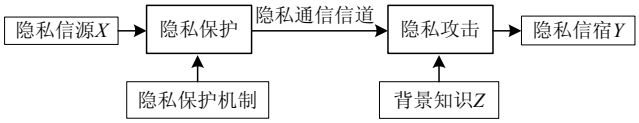


Fig.2 Communication model of privacy protection with single privacy information source and adversaries' attacks

图 2 含敌手攻击的单隐私信源隐私保护通信模型

在该模型中,Z 表示背景知识空间,其数学模型亦可定义为

$$\begin{pmatrix} Z \\ P(Z) \end{pmatrix}=\begin{pmatrix} z_1 & z_2 & \ldots & z_k & \ldots & z_l \\ p(z_1) & p(z_2) & \ldots & p(z_k) & \ldots & p(z_l) \end{pmatrix},\ 0\leqslant p(z_k)\leqslant 1,\ \sum_{k=1}^{l}p(z_k)=1,\ k=1,2,...,l \tag{6}$$

攻击者可以利用背景知识 Z 加强对隐私进行攻击,对于攻击者来说,可以联合隐私信宿消息 Y 和背景知识 Z 进行隐私分析攻击,引入攻击条件熵:

$$H(X/YZ)=-\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l}p(x_iy_jz_k)\log_2 p(x_i/y_jz_k) \tag{7}$$

$H(X/YZ)$反映了攻击者在获得隐私信宿消息 Y 和背景知识 Z 后,关于 X 仍然存在的不确定度,它实际上可以作为在某攻击手段下隐私信息的不确定度,也可以作为隐私保护强度的度量.类似地,进一步定义隐私攻击平均互信息:

$$I(X;Y/Z)=\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l}p(x_iy_jz_k)\log_2\frac{p(x_iz_k/y_j)}{p(x_i/z_k)p(y_j/z_k)} \tag{8}$$

$I(X;Y/Z)$反映了得到 Z 的条件下,X 和 Y 之间的平均互信息量,即接收方获得的隐私信息量,亦可刻画具有背景知识攻击下的隐私泄露程度.

2.3 带主观感受的信息熵模型

现实中的隐私信息的敏感性通常带有主观性,不同的人对隐私信息的价值感受不同.本节将权重引入前两节的信息熵模型中,提出含有主观感受的信息熵模型及度量.

(1) 带主观感受的隐私保护信息熵模型

针对图 1 所述通信模型的隐私消息 $x_i(i=1,2,\ldots,n)$,设置一个非负实数作为该消息的敏感程度权值,权值越大,敏感程度就越大,权值空间如下:

$$\begin{pmatrix} X \\ W(X) \end{pmatrix}=\begin{pmatrix} x_1 & x_2 & \ldots & x_i & \ldots & x_n \\ w_1 & w_2 & \ldots & w_i & \ldots & w_n \end{pmatrix},\ w_i\geqslant 0,\ i=1,2,...,n \tag{9}$$

定义隐私加权信源熵:

$$H_w(X)=-\sum_{i=1}^{n}w_ip(x_i)\log_2 p(x_i) \tag{10}$$

$H_w(X)$是通过权重 $w_i(i=1,2,\ldots,n)$来刻画不同用户对隐私消息的主观敏感性,以此实现带主观感受的隐私信息度量.隐私信源加权熵显然有以下性质:

1) 非负性.表示隐私信源一旦发生了一个隐私泄露事件,其总能提供一定的隐私信息.
2) 连续性.当隐私信源发生的隐私事件概率发生微小波动时,就形成另一个隐私信源,变化前后的两个隐私信源的加权熵是连续的.该特性对于刻画因时间变化而使隐私信源的特性变化是非常有效的.如在某一段时间内,一个人的生活规律是固定的,导致其能够泄露个人隐私的行为模式的概率分布是相对固定的,但随时间的推移,此人的生活规律会连续性地发生微小的变化,进而能够泄露其隐私的行为模式概率分布也发生了微小的变动.但行为发生变化前后,关于行为总体的加权熵是连续的.

此外,隐私信源加权熵还有信息熵的其他性质,在隐私保护系统中也有相应的实际意义.

同样地,可以定义隐私加权条件熵 $H_w(X/Y)$刻画隐私谋取者获取了一些隐私信息条件下,关于信息拥有者的

隐私信息平均不确定程度:

$$H_w(X/Y)=-\sum_{i=1}^{n}w_i\sum_{j=1}^{m}p(x_iy_j)\log_2 p(x_i/y_j) \tag{11}$$

定义隐私加权平均互信息 $I_w(X;Y)$刻画带主观感受的隐私信息泄露程度,在隐私保护机制的保护下,它表示隐私谋取者通过观测到隐私事件后所获取的隐私信息量:

$$I_w(X;Y)=\sum_{i=1}^{n}w_i\sum_{j=1}^{m}p(x_iy_j)\log_2\frac{p(x_i/y_j)}{p(x_i)} \tag{12}$$

这里,隐私加权条件熵和隐私加权平均互信息仅考虑了隐私信源对隐私消息的主观感受和偏好.在实际系统中,不仅是信息拥有者对自身的隐私信息有不同的主观感受,隐私谋取者对获取到的隐私信息也有不同的主观感受和偏好.故可以进一步探讨隐私通信传播模型中隐私信宿对隐私消息的主观感受并赋予权值,甚至建立刻画隐私信源和隐私信宿双方偏好的权值矩阵,定义更加符合实际的隐私加权条件熵和隐私加权平均互信息.

(2) 带主观感受并含敌手攻击的隐私保护信息熵模型

在考虑隐私拥有者对其隐私信息的主观感受或偏好的情况下,定义加权攻击条件熵 $H_w(X/YZ)$刻画隐私信宿 Y 在背景知知识 Z 支持下的攻击效果,它也可以作为隐私保护方法在敌手攻击下的保护强度度量:

$$H_w(X/YZ)=-\sum_{i=1}^{n}w_i\sum_{j=1}^{m}\sum_{k=1}^{l}p(x_iy_jz_k)\log_2 p(x_i/y_jz_k) \tag{13}$$

在此基础上,进一步定义隐私攻击加权平均互信息 $I_w(X;Y/Z)$,它表示在得到 Z 的条件下隐私信宿接收到的隐私信息量,它刻画了在具有背景知识条件下的隐私泄露度量:

$$I_w(X;Y/Z)=\sum_{i=1}^{n}w_i\sum_{j=1}^{m}\sum_{k=1}^{l}p(x_iy_jx_k')\log_2\frac{p(x_iz_k/y_j)}{p(x_i/z_k)p(y_j/z_k)} \tag{14}$$

2.4 多隐私信源的隐私保护信息熵模型

(1) 多隐私信源的隐私保护信息熵模型

现实系统中的信息拥有者往往有多个,从而涉及多个隐私信源的问题,故需要建立多隐私信源的隐私保护通信模型,以对相互关联的多个信源的隐私信息的保护和攻击进行度量.图 3 所示为无隐私攻击的多隐私信源隐私保护通信模型.

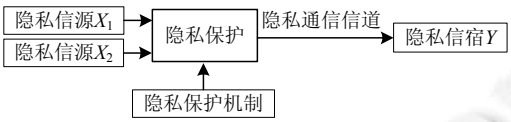


Fig.3 Communication model of privacy protection with multi-source of privacy information and none privacy attacks

图 3 无隐私攻击的多隐私信源隐私保护通信模型

在图 3 所示的通信模型中,隐私信源 X_1 和隐私信源 X_2 共同构成隐私信源 X,其数学模型为

$$\begin{pmatrix}X_1\\P(X_1)\end{pmatrix}=\begin{pmatrix}x_{11} & x_{12} & \dots & x_{1i_1} & \dots & x_{1n_1}\\ p(x_{11}) & p(x_{12}) & \dots & p(x_{1i_1}) & \dots & p(x_{1n_1})\end{pmatrix},\ 0\leqslant p(x_{i_1})\leqslant 1,\ \sum_{i_1=1}^{n_1}p(x_{i_1})=1,\ i_1=1,2,\dots,n_1 \tag{15}$$

$$\begin{pmatrix}X_2\\P(X_2)\end{pmatrix}=\begin{pmatrix}x_{21} & x_{22} & \dots & x_{2i_2} & \dots & x_{2n_2}\\ p(x_{21}) & p(x_{22}) & \dots & p(x_{2i_2}) & \dots & p(x_{2n_2})\end{pmatrix},\ 0\leqslant p(x_{i_2})\leqslant 1,\ \sum_{i_2=1}^{n_2}p(x_{i_2})=1,\ i_2=1,2,\dots,n_2 \tag{16}$$

隐私信宿 Y 的数学模型如公式(2)所述,定义多源联合隐私信源熵 $H(X_1X_2)$,该信源熵刻画的是多个带关联的隐私拥有者的隐私信息度量:

$$H(X_1X_2)=-\sum_{i_1=1}^{n_1}\sum_{i_2=1}^{n_2}p(x_{i_1}x_{i_2})\log_2 p(x_{i_1}x_{i_2})=H(X_1)+H(X_2/X_1) \tag{17}$$

已知隐私信宿 Y 条件下关于隐私信源 X 的多源联合隐私条件熵可以定义为 $H(X/Y)=H(X_1X_2/Y)=H(X_1X_2Y)-H(Y)$.该定义刻画的是多个带关联的隐私信源在实施隐私保护后,隐私信息获取者通过对隐私事件进行观测后其对多个信息拥有者私信息的平均联合不确定程度.

同时,可以定义多源联合平均互信息 $I(X_1X_2;Y)$来刻画带关联的多个隐私信源的隐私泄露程度:

$$I(X_1X_2;Y)=\sum_{i_1=1}^{n_1}\sum_{i_2=1}^{n_2}\sum_{j=1}^{m}p(x_{i_1}x_{i_2}y_j)\log_2\frac{p(x_{i_1}x_{i_2}/y_j)}{p(x_{i_1}x_{i_2})} \tag{18}$$

(2) 多隐私信源带隐私攻击的隐私保护信息熵模型

在第 2.2 节中提出的带隐私攻击隐私保护信息熵模型基础上,引入多个带关联的信息拥有者,构成新的关联的多隐私信源,构建多隐私信源带敌手攻击的隐私保护信息熵模型,如图 4 所示.

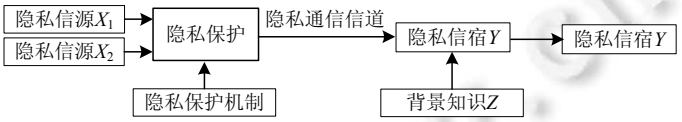


Fig.4 Communication model of privacy protection with multi-source of privacy information and attacks

图 4 带隐私攻击的多隐私信源隐私保护通信模型

图 4 所述通信模型的信源数学模型如公式(15)和公式(16),隐私信宿 Y 的数学模型如公式(2)所述.该模型下的多源联合信源熵为 $H(X)=H(X_1X_2)$,多源联合隐私攻击条件熵为 $H(X_1X_2/YZ)$,多源联合隐私攻击条件平均互信息为 $I(X_1X_2;Y/Z)$,其中,多源联合隐私攻击条件熵表示的是在背景知识攻击下接收者对联合隐私信源的隐私信息的不确定度;多源联合隐私攻击条件平均互信息表示的是在背景知识攻击下联合隐私信源的隐私泄露程度.其中,

$$\left.\begin{aligned}H(X_1X_2/YZ)&=H(X_1X_2YZ)-H(YZ)\\I(X_1X_2;Y/Z)&=H(X_1X_2)-H(X_1X_2Y/Z)\end{aligned}\right\} \tag{19}$$

3 隐私度量及其对隐私保护机制和隐私攻击手段的评价

运用信息熵和平均互信息可以对隐私信息进行相关度量,以此为基础,实现对隐私保护机制的抗攻击能力测评方法的建立.

3.1 隐私度量方法

在基本信息熵模型中,隐私条件熵 $H(X/Y)$中可用于度量在隐私保护机制下,隐私信源仍存在的不确定程度,从而其可以评测隐私保护算法的强度.若记 P_i 为某一具体隐私保护算法,则 $H_{P_i}(X/Y)$ 就是在用 P_i 实施保护后隐私信宿(敌手)Y 仍对隐私的未知量,从隐私拥有者的角度来说,希望该条件熵尽可能地大.而隐私平均互信息 $I(X;Y)$表示的是隐私信宿 X 在隐私保护机制的保护下,被信宿 Y 所获取的平均隐私信息量,同样地, $I_{P_i}(X;Y)$ 就是在用 P_i 实施保护后信宿 Y 接收到的隐私信息,它应越小越好.

性质 1. 隐私条件熵 $H(X/Y)$和隐私互信息 $I(X;Y)$具有隐私度量的一致性.

证明:由公式(5)可知:

$$\begin{aligned}I(X;Y)&=\sum_{i=1}^{n}\sum_{j=1}^{m}p(x_iy_j)\log_2\frac{p(x_i/y_j)}{p(x_i)}\\&=\sum_{i=1}^{n}\sum_{j=1}^{m}p(x_iy_j)\log_2\frac{1}{p(x_i)}-\sum_{i=1}^{n}\sum_{j=1}^{m}p(x_iy_j)\log_2\frac{1}{p(x_i/y_j)}\\&=\sum_{i=1}^{n}p(x_i)\log_2\frac{1}{p(x_i)}-\sum_{i=1}^{n}\sum_{j=1}^{m}p(x_iy_j)\log_2\frac{1}{p(x_i/y_j)}\\&=H(X)-H(X/Y)\end{aligned} \tag{20}$$

故有 $I(X;Y)=H(X)-H(X/Y)$,因此,隐私条件熵越大,则隐私平均互信息就越小,它们具有一致性. □

在含敌手攻击的隐私保护信息熵模型中,隐私度量主要包括在敌手攻击下信源本身含有的隐私信息量、敌手的攻击能力、隐私保护算法强度和隐私泄露程度.其中,信源本身含有的隐私信息量可用隐私信源熵 $H(X)$的大小来描述,其表示信息拥有者隐私信息的固有量大小,一旦信源确定,则此信源所拥有的隐私信息量就是一个确定的值;而敌手的攻击能力和隐私保护算法强度可用 $H(X/YZ)$度量,对于敌手 Y 来说,它表示敌手在背景知识的攻击下,对信源隐私信息的不确定程度,也是隐私保护算法的保护强度;敌手在背景知识的攻击下所造成的隐私泄露程度可以用平均隐私互信息量 $I(X;Y/Z)$表示,根据性质 1,它也可以度量敌手的攻击能力和隐私保护算法强度.若记敌手在背景知识下的攻击手段为 A_r、保护算法为 P_i,则 $H_{P_i,A_r}(X/YZ)$ 和 $I_{P_i,A_r}(X;Y/Z)$ 均可度量 A_r 的能力、P_i 的强度和系统在抵抗 A_r 攻击下采用 P_i 的隐私信息泄露程度.

相应地,带主观感受的隐私保护信息熵模型、带主观感受并含敌手攻击的隐私保护信息熵模型、多隐私信源的隐私保护信息熵模型和多隐私信源带隐私攻击的隐私保护信息熵模型这 4 个模型中的隐私度量,可以在上述讨论的基础上,运用相应的隐私信息熵或互信息量实现.其中,加权隐私信源熵 $H_w(X)$和多源联合信源熵 $H(X_1X_2)$可用于度量隐私信源的固有隐私量;$H_w(X/YZ)$和 $I_w(X;Y/Z)$可用于度量带主观感受并含敌手攻击的隐私保护信息熵模型中的敌手的攻击能力、隐私保护算法强度和隐私泄露程度;$H(X_1X_2/YZ)$和 $I(X_1X_2;Y/Z)$可用于度量多隐私信源带隐私攻击的隐私保护信息熵模型中的敌手的攻击能力、隐私保护算法强度和隐私泄露程度.特别地,性质 1 所述的隐私度量性质在这些隐私保护信息熵模型中仍成立.

3.2 隐私保护机制及隐私攻击评价分析

(1) 隐私保护基本信息熵模型下的隐私保护机制评价分析

运用隐私保护机制(算法)对信息拥有者的隐私信息进行保护,目的是使 $H(X/Y)$尽可能地小,即希望通过某种隐私保护机制,使得隐私谋取者得到的信息量 $I(X;Y)$尽可能地小,最好是 0.

定义 1. 若在某种隐私保护机制的保护下,隐私平均互信息 $I(X;Y)=0$(隐私信宿从隐私信源接收到的隐私信息量为 0),则称该隐私保护机制对此信源是完全隐私保护的.

定义 2. 对同一隐私信源 X,分别采用隐私保护机制 P_i 和 P_j 进行保护:

- 若 $H_{P_i}(X/Y)<H_{P_j}(X/Y)$ 或 $I_{P_i}(X;Y)>I_{P_j}(X;Y)$,则称隐私保护机制 P_j 比 P_i 隐私保护有效性好,简记为偏序关系 $P_i \prec P_j$;
- 若 $H_{P_i}(X/Y)=H_{P_j}(X/Y)$ 或 $I_{P_i}(X;Y)=I_{P_j}(X;Y)$,则称隐私保护机制 P_i 与 P_j 隐私保护有效性等价,简记为等价关系 $P_i \cong P_j$.

定理 1. 设隐私保护机制有效性偏序关系与等价关系如定义 2 所定义,则偏序关系具有可传递性,等价关系具有自反性、可传递性和对称性.

证明:若有 $P_i \prec P_j, P_j \prec P_k$,则按照定义有 $H_{P_i}(X/Y)<H_{P_j}(X/Y)$ 和 $H_{P_j}(X/Y)<H_{P_k}(X/Y)$,根据信息熵的性质,易得 $H_{P_i}(X/Y)<H_{P_k}(X/Y)$,即 $P_i \prec P_k$.同样地,若 $I_{P_i}(X;Y)>I_{P_j}(X;Y)$ 和 $I_{P_j}(X;Y)>I_{P_k}(X;Y)$,根据性质 1,易证 $I_{P_i}(X;Y)>I_{P_k}(X;Y)$,进而有 $P_i \prec P_k$.即偏序关系有可传递性.类似地,易证等价关系的 3 个特性. □

定义 3(隐私保护有效性距离). 在隐私保护基本信息熵模型中,对同一隐私信源 X 分别采用隐私保护机制 P_i 和 P_j 进行保护,若隐私信宿 Y 接收到的隐私信息量分别为 $I_{P_i}(X;Y)$ 和 $I_{P_j}(X;Y)$,则这两种隐私保护机制的有效性距离定义为 $d_I=|I_{P_i}(X;Y)-I_{P_j}(X;Y)|$.

在隐私保护基本信息熵模型中,隐私保护有效性距离刻画的是保护同一隐私信息的两种不同隐私保护机制有效性差异大小.显然,d_I越小,两种隐私保护算法的有效性差异越小;d_I越大,两种隐私保护算法的有效性差异越大.

(2) 含敌手攻击的隐私保护机制及隐私攻击评价分析

在实际系统中,隐私保护机制的目标是:在遭受敌手各类隐私攻击的情况下,仍然使信息拥有者的隐私信息

尽可能少地被隐私谋取者所获得.即希望通过某种隐私保护机制抵抗敌手在一定背景知识下的隐私攻击,使得隐私谋取者得到的隐私信息量 $I(X;Y/Z)$尽可能地小,最好是 0.

定义 4. 对于带敌手攻击的隐私保护系统,若 $I(X;Y/Z)=0$,即在敌手在拥有背景知识 Z 的攻击下,若隐私保护机制能够使信息拥有者的隐私信息泄露量为 0,则称隐私系统是完美隐私保护的.

定义 5. 对于带敌手攻击的隐私保护系统,若敌手采用隐私攻击手段 A_r进行攻击,系统分别采用隐私保护机制 P_i 和 P_j 进行保护:

- 若 $H_{P_i,A_r}(X/YZ)<H_{P_j,A_r}(X/YZ)$ 或 $I_{P_i,A_r}(X;Y/Z)>I_{P_j,A_r}(X;Y/Z)$,则称在抵抗 A_r 攻击时,隐私保护机制 P_j 比 P_i 隐私保护有效性好,记为偏序关系 $P_i(A_r)\prec P_j(A_r)$;
- 若 $H_{P_i,A_r}(X/YZ)=H_{P_j,A_r}(X/YZ)$ 或 $I_{P_i,A_r}(X;Y/Z)=I_{P_j,A_r}(X;Y/Z)$,则称隐私保护机制 P_i 与 P_j 隐私保护有效性等价,简记为 $P_i(A_r)\cong P_j(A_r)$.

定义 6(抗隐私攻击的隐私保护有效性距离). 在含敌手攻击的隐私保护信息熵模型中,对同一隐私信源 X 和针对该信源的隐私攻击 A_r,若在该隐私攻击下分别采用隐私保护机制 P_i 和 P_j 进行保护,隐私信宿 Y 获取的隐私信息量分别为 $I_{P_i,A_r}(X;Y/Z)$ 和 $I_{P_j,A_r}(X;Y/Z)$,则称这两种隐私保护机制在隐私攻击 A_r 下的有效性距离为

$$d_I(A_r)=|I_{P_i,A_r}(X;Y/Z)-I_{P_j,A_r}(X;Y/Z)|.$$

在含敌手攻击的隐私保护信息熵模型中,抗隐私攻击的隐私保护有效性距离 $d_I(A_r)$刻画的是不同隐私保护机制在同一种隐私攻击下的有效性差异大小.

定义 7. 在同一隐私保护机制 P_i 下,敌手采用隐私攻击 A_r 和 A_q 进行攻击:

- 若 $H_{P_i,A_r}(X/YZ)<H_{P_i,A_q}(X/YZ)$ 或 $I_{P_i,A_r}(X;Y/Z)>I_{P_i,A_q}(X;Y/Z)$,则称在隐私保护机制 P_i 的保护下,隐私攻击 A_r 比 A_q 的有效性更强,简记为偏序关系 $A_r(P_i)\succ A_q(P_i)$;
- 若 $H_{P_i,A_r}(X/YZ)=H_{P_j,A_r}(X/YZ)$ 或 $I_{P_i,A_r}(X;Y/Z)=I_{P_j,A_r}(X;Y/Z)$,则称在隐私保护机制 P_i 的保护下,隐私攻击 A_r 与隐私攻击 A_q 的隐私攻击有效性等价,简记为 $A_r(P_i)\cong A_q(P_i)$.

定理 2. 若偏序关系和等价关系如定义 5 或定义 7,则偏序关系$\prec$满足传递性,等价关系$\cong$满足自反性、对称性和可传递性.

证明:与定理 1 的证明类似,略. □

定义 8(隐私攻击有效性距离). 在含敌手攻击的隐私保护信息熵模型中,在同一隐私保护机制 P_i 下,敌手采用隐私攻击 A_r 和 A_q 进行攻击,则称这两种隐私攻击的有效性距离为 $d_I(P_i)=|I_{P_i,A_r}(X;Y)-I_{P_i,A_q}(X;Y)|$.

在含敌手攻击的隐私保护信息熵模型中,隐私攻击有效性距离 $d_I(P_i)$刻画的是敌手攻击能力的差异性,它给出了敌手攻能力的度量.

另外,在隐私保护系统中,隐私互信息可以刻画含背景知识与否时隐私泄露程度大小.一般地,敌手获得背景知识后,总是可以获得一定的隐私信息.

定理 3. 在带敌手攻击的隐私保护通信模型中,假设敌手的背景知识为 Z,则 $I(X;Y)\leqslant I(X;YZ)$.

证明:由平均互信息的计算方程可知:

$$I(X;Y)=H(X)-H(X/Y) \tag{21}$$

$$I(X;YZ)=H(X)-H(X/YZ) \tag{22}$$

令公式(22)减去公式(21),得到:

$$I(X;YZ)-I(X;Y)=H(X/Y)-H(X/YZ) \tag{23}$$

由信息熵性质有 $H(X/Y)\geqslant H(X/YZ)$,故 $H(X/Y)-H(X/YZ)\geqslant 0$,$I(X;YZ)\geqslant I(X;Y)$. □

该定理说明:敌手在一定背景知识下进行隐私攻击与分析,敌手所获得的隐私信息不少于其无背景知识情况下所能获得的隐私信息.这也为隐私保护提供了一个方向,即,使敌手截取的隐私消息与其拥有背景知识关联程度尽可能地小,从而最大限度地保护隐私信息.

(3) 其他隐私保护信息熵模型下的隐私保护机制及隐私攻击评价分析

前面已分析了隐私保护基本信息熵模型和含敌手攻击的信息熵模型的隐私保护机制强度及隐私攻击能力,以此为基础,其分析方法可以扩展到带主观感受并含敌手攻击的隐私保护信息熵模型、多隐私信源的隐私保护信息熵模型和多隐私信源带隐私攻击的隐私保护信息熵模型.这几个模型所涉及到的隐私熵有加权隐私信源熵 $H_w(X)$、多源联合信源熵 $H(X_1X_2)$、条件熵 $H_w(X/YZ)$和 $H(X_1X_2/YZ)$以及隐私互信息量有 $I_w(X;Y/Z)$和 $I(X_1X_2;Y/Z)$.根据信息熵的有关性质,以它们为基础可以将定义 1~定义 8、定理 1~定理 3 相应地推广或扩展到这几个模型中.

4 实例分析

前面所提出的隐私保护信息熵模型及其度量方法属于通用情形,可适用于不同应用场景.下面以一个简单的位置隐私保护应用为实例对该模型进行有效性分析.假设某用户 u 在一个被划分为 M 块的区域内移动,记 $R=\{r_1,r_2,\ldots,r_M\}$为 M 块不同区域的集合,即位置空间,攻击者的目的是确定该用户所在的真实位置.

4.1 位置隐私保护的通信模型

对应于含敌手攻击的隐私保护信息熵模型,隐私信源为用户可能所处的位置分布 R,随机变量 R 的取值表示用户 u 处于某一位置区域 r_i,用$\{r_1,r_2,\ldots,r_M\}$表示用户所处的位置区域空间,假设各区域的概率为 $p(r_i)$,有 $0\leqslant p(r_i)\leqslant 1, \sum_{i=1}^{M} p(r_i)=1$,则 R 的概率模型可以表示为

$$\begin{pmatrix} R \\ P(R) \end{pmatrix}=\begin{pmatrix} r_1 & r_2 & \ldots & r_i & \ldots & r_M \\ p(r_1) & p(r_2) & \ldots & p(r_i) & \ldots & p(r_M) \end{pmatrix}. \tag{24}$$

用户的真实位置分布信息是隐私信息,为防止攻击者直接获取用户所处的真实区域,需要对用户的位置分布 R 进行保护,经过位置隐私保护机制(包括位置泛化、取假名、隐藏或添加虚拟位置等)对位置分布 R 进行隐私保护处理后,变成可被攻击者直接观察到的可观察位置分布 R',设 $R'=\{r_1',r_2',\ldots,r_{M'}'\}$,其中,$r_i'$ 表示用户 u 的经过隐私保护后可被攻击者观察到的所在区域,可观察位置分布 R'的概率模型为

$$\begin{pmatrix} R' \\ P(R') \end{pmatrix}=\begin{pmatrix} r_1' & r_2' & \ldots & r_i' & \ldots & r_{M'}' \\ p(r_1') & p(r_2') & \ldots & p(r_i') & \ldots & p(r_{M'}') \end{pmatrix},\ 0\leqslant p(r_i')\leqslant 1,\ \sum_{i=1}^{M'} p(r_i')=1. \tag{25}$$

攻击者获取到可观察位置分布 R'后,结合背景知识对用户 u 进行位置攻击,即得到攻击者对用户 u 的推断位置 $\hat{R}$,设 $\hat{R}=\{\hat{r}_1,\hat{r}_2,\ldots,\hat{r}_{\hat{M}}\}$,其中,$\hat{r}_i$ 表示攻击者猜测用户 u 所处区域为真实区域,其概率模型为

$$\begin{pmatrix} \hat{R} \\ P(\hat{R}) \end{pmatrix}=\begin{pmatrix} \hat{r}_1 & \hat{r}_2 & \ldots & \hat{r}_i & \ldots & \hat{r}_{\hat{M}} \\ p(\hat{r}_1) & p(\hat{r}_2) & \ldots & p(\hat{r}_i) & \ldots & p(\hat{r}_{\hat{M}}) \end{pmatrix},\ 0\leqslant p(\hat{r}_i)\leqslant 1,\ \sum_{i=1}^{\hat{M}} p(\hat{r}_i)=1. \tag{26}$$

图 5 表示位置隐私保护场景的通信模型,可以看作含敌手攻击的隐私保护信息熵模型的一个具体实例.

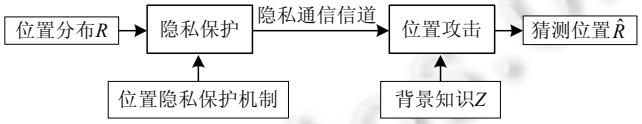


Fig.5 Communication model of location privacy protection

图 5 位置隐私保护通信模型

4.2 相同背景知识下不同隐私保护机制的效果比较

在初始阶段,用户 u 处于一个真实区域 r_i,则该用户处于区域 r_i 的概率为 1,处于其他区域的概率为 0.具体为

$$\begin{pmatrix} R \\ P(R) \end{pmatrix}=\begin{pmatrix} r_1 & r_2 & \ldots & r_i & \ldots & r_M \\ 0 & 0 & \ldots & 1 & \ldots & 0 \end{pmatrix}. \tag{27}$$

此时,隐私信源熵即位置分布 R 的熵为 $H(R)=-\sum_{i=1}^{M} p(r_i)\log p(r_i)=0$.

(1) 弱隐私保护强度的隐私度量

如果采用位置泛化作为位置隐私保护机制,若将用户 u 的发布位置从区域 r_i 泛化到$\{r_{i-1},r_i,r_{i+1},r_{i+2}\}$,可得到可观察位置分布的概率模型如下:

$$\begin{pmatrix} R' \\ P(R') \end{pmatrix}=\begin{pmatrix} r'_1 & \cdots & r'_{i-1} & r'_i & r'_{i+1} & r'_{i+2} & \cdots & r'_{M'} \\ 0 & \cdots & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \cdots & 0 \end{pmatrix}, \tag{28}$$

则可观察位置分布的熵为 $H(R')=-\sum_{i=1}^{M'}p(r'_i)\log p(r'_i)=2$, 等同于含敌手攻击的隐私保护信息熵模型下的熵 $H(X/Y)$.

攻击者在获取到可观察位置分布后,结合其所拥有的背景知识进行分析,在一定的背景知识下,分析出用户 u 的推断位置分布概率模型如下:

$$\begin{pmatrix} \hat{R} \\ P(\hat{R}) \end{pmatrix}=\begin{pmatrix} \hat{r}_1 & \cdots & \hat{r}_{i-1} & \hat{r}_i & \hat{r}_{i+1} & \hat{r}_{i+2} & \cdots & \hat{r}_{\hat{M}} \\ 0 & \cdots & \frac{1}{4} & \frac{1}{4} & \frac{1}{8} & \frac{1}{8} & \cdots & 0 \end{pmatrix}. \tag{29}$$

此时我们可得 $H(\hat{R})=-\sum_{i=1}^{\hat{M}}p(\hat{r}_i)\log p(\hat{r}_i)=1.75$, 它表示攻击者在具有背景知识的条件下对用户所在位置的不确定程度,等同于敌手攻击的隐私保护信息熵模型下的熵 $H(X/YZ)$.

(2) 强隐私保护强度的隐私度量

当我们取泛化位置区域变大时,即隐私保护手段变强后,我们取用户 u 的发布位置从区域$\{r_{i-1},r_i,r_{i+1},r_{i+2}\}$变到$\{r_i,r_{i+1},\ldots,r_{i+7}\}$,可观察位置分布的概率模型为

$$\begin{pmatrix} R' \\ P(R') \end{pmatrix}=\begin{pmatrix} r'_1 & \cdots & r'_i & \cdots & r'_{i+7} & \cdots & r'_{M'} \\ 0 & \cdots & \frac{1}{8} & \cdots & \frac{1}{8} & \cdots & 0 \end{pmatrix}, \tag{30}$$

则 $H(R')=-\sum_{i=1}^{M'}p(r'_i)\log p(r'_i)=3$,表示可观察位置分布的熵.攻击者在相同的背景知识下,分析得到对用户 u 的推断位置分布的概率模型如下:

$$\begin{pmatrix} \hat{R} \\ P(\hat{R}) \end{pmatrix}=\begin{pmatrix} \hat{r}_1 & \cdots & \hat{r}_i & \hat{r}_{i+1} & \hat{r}_{i+2} & \hat{r}_{i+3} & \hat{r}_{i+4} & \hat{r}_{i+5} & \hat{r}_{i+6} & \hat{r}_{i+7} & \cdots & \hat{r}_{M'} \\ 0 & \cdots & \frac{1}{2} & \frac{1}{8} & \frac{1}{8} & \frac{1}{16} & \frac{1}{16} & \frac{1}{16} & \frac{1}{32} & \frac{1}{32} & \cdots & 0 \end{pmatrix}. \tag{31}$$

此时,我们可得 $H(\hat{R})=-\sum_{i=1}^{\hat{M}}p(\hat{r}_i)\log p(\hat{r}_i)=2.3125$, 表示攻击者在具有背景知识的条件下对用户所在位置的不确定度的度量,等同于敌手攻击的隐私保护信息熵模型下的熵 $H(X/YZ)$.

由 2.3125>1.75 可验证含敌手攻击的隐私保护信息熵模型下 $H_{P_i,A_r}(X/YZ)<H_{P_j,A_r}(X/YZ)$ 成立.

4.3 相同隐私保护机制下不同隐私攻击的效果比较

(1) 弱隐私攻击强度的隐私度量

同第 4.2 节弱隐私保护强度的隐私度量.

(2) 强隐私攻击强度的隐私度量

隐私保护机制同第 4.2 节弱隐私保护强度的隐私度量,攻击者在获取到可观察位置分布后,结合其所拥有的背景知识进行分析,在强隐私攻击强度下,分析得到对用户 u 的更准确的推断位置分布的概率模型如下:

$$\begin{pmatrix} \hat{R} \\ P(\hat{R}) \end{pmatrix}=\begin{pmatrix} \hat{r}_1 & \cdots & \hat{r}_{i-1} & \hat{r}_i & \hat{r}_{i+1} & \hat{r}_{i+2} & \cdots & \hat{r}_{M'} \\ 0 & \cdots & \frac{1}{6} & \frac{2}{3} & \frac{1}{12} & \frac{1}{12} & \cdots & 0 \end{pmatrix}. \tag{32}$$

此时,我们可得 $H(\hat{R})=-\sum_{i=1}^{\hat{M}}p(\hat{r}_i)\log p(\hat{r}_i)=1.418$, 表示攻击者在具有背景知识的条件下对用户所在位置的不确定度的度量,等同于敌手攻击的隐私保护信息熵模型下的熵 $H(X/YZ)$.

由 1.418<1.75 可验证含敌手攻击的隐私保护信息熵模型下 $H_{P_i,A_r}(X/YZ)<H_{P_i,A_q}(X/YZ)$ 成立.

5 结 论

本文基于 Shannon 信息论提出了几种隐私保护信息熵模型,其关键出发点是将隐私保护系统视为一种通信模型,通过定义信源、信宿和信道/引入信息熵、平均互信息量、条件熵及条件互信息等概念,初步给出了不同场合的隐私信息度量、隐私泄露度量、隐私保护强度量化和攻击能力量化等方法,并且初步考虑了含隐私信息主观感受的信息熵模型.本文的工作虽然只给出了较为基本的信息熵模型,但为解决隐私保护系统的量化问题建立了一个可行的体系基础,相信在信息论相关成果的支撑下,其相关研究可以不断深入,包括连续隐私信源的研究、更复杂的多隐私信源模型、基于随机过程的信息熵模型、贝叶斯隐私信息熵模型和马尔柯夫隐私信息熵模型等,都具备了深入研究的可行性.同时,由于隐私信息带有时空性、主观性、模糊性,下一步拟考虑采用广义信息论、模糊信息论等研究隐私信息熵模型.

References:

[1] Kelly DJ, Raines RA, Grimaila MR, Baldwin RO, Mullins BE. A survey of state-of-the-art in anonymity metrics. In: Antonatos S, ed. Proc. of the 1st ACM Workshop on Network Data Anonymization. Alexandria: ACM Press, 2008. 31–40. [doi: 10.1145/1456441.1456453]

[2] Shokri R, Theodorakopoulos G, Le Boudec JY, Hubaux JP. Quantifying location privacy. In: Frincke D, ed. Proc. of the 2011 IEEE Symp. on Security and Privacy. Berkeley: IEEE, 2011. 247–262. [doi: 10.1109/SP.2011.18]

[3] Wang CM, Guo YJ, Guo YH. Privacy metric for user's trajectory in location-based services. Ruan Jian Xue Bao/Journal of Software, 2012,23(2):352−360 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3946.htm [doi: 10.3724/SP.J.1001.2012.03946]

[4] Chen Y. Information Theroy and Coding. 2nd ed., Beijing: Publishing House of Electronics Industry, 2012 (in Chinese).

[5] Díaz C, Seys S, Claessens J, Preneel B. Towards measuring anonymity. In: Dingledine R, Syverson P, eds. Proc. of the 2nd Int'l Conf. on Privacy Enhancing Technologies. Berlin, Heidelberg: Springer-Verlag, 2002. 54−68. [doi: 10.1007/3-540-36467-6_5]

[6] Serjantov A, Danezis G. Towards an information theoretic metric for anonymity. In: Dingledine R, Syverson P, eds. Proc. of the 2nd Int'l Conf. on Privacy Enhancing Technologies. Berlin, Heidelberg: Springer-Verlag, 2002. 41−53. [doi: 10.1007/3-540-36467-6_4]

[7] Wagner I, Eckhoff D. Technical privacy metrics: A systematic survey. arXiv preprint arXiv:1512.00327, 2015.

[8] Shannon CE. A mathematical theory of communication. Bell System Technical Journal, 1948,27(3):379−423. [doi: 10.1002/j.1538-7305.1948.tb01338.x]

[9] Hoh B, Gruteser M, Xiong H, Alrabady A. Preserving privacy in GPS traces via uncertainty-aware path cloaking. In: Ning P, ed. Proc. of the 14th ACM Conf. on Computer and Communications Security. Alexandria: ACM Press, 2007. 161−171. [doi: 10.1145/1315245.1315266]

[10] Hoh B, Gruteser M, Herring R, Ban J, Work D, Herrera JC, Bayen A, Annavaram M, Jacobson Q. Virtual trip lines for distributed privacy-preserving traffic monitoring. In: Proc. of the 6th Int'l Conf. on Mobile Systems, Applications, and Services. New York: ACM Press, 2008. 15−28. [doi: 10.1145/1378600.1378604]

[11] Ma Z, Kargl F, Weber M. Measuring location privacy in V2X communication systems with accumulated information. In: Ni LM, ed. Proc. of the 6th IEEE Int'l Conf. on Mobile Ad-Hoc and Sensor Systems. Macao: IEEE, 2009. 322−331. [doi: 10.1109/MOBHOC.2009.5336983]

[12] Lin X, Li SP, Yang CH. Attacking algorithms against continuous queries in LBS and anonymity measurement. Ruan Jian Xue Bao/Journal of Software, 2009,20(4):1058−1068 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3428.htm [doi: 10.3724/SP.J.1001.2009.03428]

[13] Chen X, Pang J. Measuring query privacy in location-based services. In: Bertino E, ed. Proc. of the 2nd ACM Conf. on Data and Application Security and Privacy. New York: ACM Press, 2012. 49−60. [doi: 10.1145/2133601.2133608]

[14] Niu B, Li QH, Zhu XY, Cao GH, Li H. Achieving *k*-anonymity in privacy-aware location-based services. In: Alberto LG, ed. Proc. of the 2014 IEEE Conf. on Computer Communications. Toronto: IEEE, 2014. 754−762. [doi: 10.1109/INFOCOM.2014.6848002]

[15] Zhang XJ, Gui XL, Feng ZC, Tian F, Yu S, Zhao JQ. A quantifying framework of query privacy in location-based service. Journal of Xi'an Jiaotong University, 2014,48(2):8−13 (in Chinese with English abstract).

[16] Ngoc TH, Echizen I, Komei K, Yoshiura H. New approach to quantification of privacy on social network sites. In: Chang E, Barolli L, eds. Proc.of the 24th IEEE Int'l Conf. on Advanced Information Networking and Applications. Perth: IEEE, 2010. 556−564. [doi: 10.1109/AINA.2010.118]

[17] Yang YH, Lutes J, Li FJ, Luo B, Liu P. Stalking online: On user privacy in social networks. In: Bertino E, ed. Proc. of the 2nd ACM Conf. on Data and Application Security and Privacy. New York: ACM Press, 2012. 37−48. [doi: 10.1145/2133601.2133607]

[18] Agrawal D, Aggarwal CC. On the design and quantification of privacy preserving data mining algorithms. In: Proc. of the 20th ACM SIGMOD-SIGACT-SIGART Symp. on Principles of Database Systems. New York: ACM Press, 2001. 247−255. [doi: 10.1145/375551.375602]

[19] Bertino E, Lin D, Jiang W. A survey of quantification of privacy preserving data mining algorithms. In: Proc. of the Privacy-Preserving Data Mining. Springer-Verlag, 2008. 183−205. [doi: 10.1007/978-0-387-70992-5_8]

[20] Edman M, Sivrikaya F, Yener B. A combinatorial approach to measuring anonymity. In: Merusan G, Altiok T, Melamed B, Zeng D, eds. Proc. of the 2007 Intelligence and Security Informatics. New Brunswick: IEEE, 2007. 356−363. [doi: 10.1109/ISI.2007.379497]

[21] Liu D, Bagh A. New privacy-preserving ascending auction for assignment problems. In: Ramnath K, Marius FN, German FR, Wu DJ, eds. Proc. of the 2016 Theory in Economics of Information Systems. Costa Rica, 2016. 1−23.

附中文参考文献:

[3] 王彩梅,郭亚军,郭艳华.位置服务中用户轨迹的隐私度量.软件学报,2012,23(2):352−360. http://www.jos.org.cn/1000-9825/3946.htm [doi: 10.3724/SP.J.1001.2012.03946]

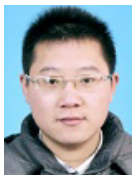
[4] 陈运.信息论与编码.第 2 版,北京:电子工业出版社,2012.

[12] 林欣,李善平,杨朝晖.LBS 中连续查询攻击算法及匿名性度量.软件学报,2009,20(4):1058−1068. http://www.jos.org.cn/1000-9825/3428.htm [doi: 10.3724/SP.J.1001.2009.03428]

[15] 张学军,桂小林,冯志超,田丰,余思,赵建强.位置服务中的查询隐私度量框架研究.西安交通大学学报,2014,48(2):8−13.

彭长根(1963－),男,贵州锦屏人,博士,教授,博士生导师,CCF 专业会员,主要研究领域为密码学,信息安全,大数据隐私保护.

丁红发(1988－),男,博士生,讲师,CCF 专业会员,主要研究领域为密码协议,数据安全.



朱义杰(1989－),男,硕士,主要研究领域为密码学,可信计算.

田有亮(1982－),男,博士,教授,主要研究领域为理性密码协议,数据安全.

符祖峰(1978－),男,博士生,副教授,主要研究领域为安全多方计算,机器学习.