计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.20200843
59(2):390-402,2022

基于深度学习的位置隐私攻击

沈钲晨　张千里　张超凡　唐翔宇　王继龙
(清华大学网络科学与网络空间研究院　北京　100084)
(szc18@mails.tsinghua.edu.cn)

Location Privacy Attack Based on Deep Learning

Shen Zhengchen, Zhang Qianli, Zhang Chaofan, Tang Xiangyu, and Wang Jilong
(*Institute for Network Sciences and Cyberspace*, *Tsinghua University*, *Beijing* 100084)

Abstract　With the continuous development of location services, location privacy protection has become a hotspot in privacy protection research. At present, a series of location privacy protection schemes have been proposed, most of which are based on spatial disturbance technology. However, the existing research on location privacy protection has two problems: First of all, most of the location privacy protection schemes do not consider the complicated correlation between the trajectory points of a single trajectory when performing spatial disturbances, and they usually underestimate the risk of cracking desensitization trajectories; Secondly, there is a lack of quantitative measurement of the risk of cracking the desensitization trajectory. Although differential privacy has made considerable efforts in this regard, the existence of complex relationships makes the model may not be able to objectively describe the degree of privacy protection. If the cracking risk of data after privacy protection cannot be quantified, a quantitative evaluation index cannot be established for the privacy protection scheme. Therefore, first of all, the location information with the association relationship is used to attack the desensitization trajectory. Specifically, the Markov attack algorithms using simple association relationships and the deep neural network attack algorithms using complex association relationships are designed in this paper. Secondly, the cracking risk of desensitization trajectory is quantified, and a quantitative evaluation scheme is established to evaluate the threat degree of attack algorithm to privacy protection scheme. Finally, these two kinds of attack algorithms are used to attack Geo-Indistinguishability privacy protection scheme, and the attack effect is evaluated. The results show that Geo-Indistinguishability privacy protection scheme can resist the attack of the Markov attack algorithm, but can not resist the attack of deep neural network attack algorithm.

Key words　location privacy; location privacy attack; deep learning; privacy risk assessment; time series

摘　要　随着位置服务的不断发展,位置隐私保护已成为隐私保护研究的一个热点.当前已经提出了一系列位置隐私保护方案,这些隐私保护方案大多是基于空间扰动技术来实现的.然而,现有的位置隐私保护研究存在2方面的问题:首先大部分位置隐私保护方案在进行空间扰动时,未考虑用户轨迹点间

收稿日期:2020-10-19;**修回日期**:2021-03-12
基金项目:国家重点研发计划项目(2017YFB0503703)
This work was supported by the National Key Research and Development Program of China (2017YFB0503703).
通信作者:张千里(zhang@cernet.edu.cn)

复杂的关联关系,这样的位置隐私保护方案通常会低估脱敏轨迹的破解风险;其次,脱敏轨迹的破解风险缺乏量化的度量,尽管差分隐私在这一方面做了相当的努力,然而复杂关联关系的存在使得该模型未必能够客观地描述隐私保护的程度.如果不能量化脱敏轨迹的破解风险,也就不能对隐私保护方案建立一个定量的评估指标.因此,首先利用具有关联关系的位置信息,分别设计了利用简单关联关系的Markov攻击算法和利用复杂关联关系的深度神经网络攻击算法,对脱敏轨迹进行了攻击;其次对脱敏轨迹的破解风险进行量化,建立了一个定量的评估方案,用于评估攻击算法对隐私保护方案的威胁程度;最后将这2类攻击算法对Geo-Indistinguishability隐私保护方案进行了攻击,并对攻击效果进行了评估,结果表明Geo-Indistinguishability隐私保护方案抵御了Markov攻击算法的攻击,但未能抵御深度神经网络攻击算法的攻击.

关键词 位置隐私;位置隐私攻击;深度学习;隐私风险评估;时间序列

中图法分类号 TP311

随着互联网的发展,入网人数日益增多,特别是移动端设备的普及,使得基于位置的服务已成为人们生活不可缺少的一部分.基于位置的服务[1]是一种围绕地理位置的服务,其利用各种定位技术来得到设备的当前位置并发送给服务端,服务端通过该设备发送的位置信息在空间数据库中检索与该位置相关的资源和信息反馈给设备,从而为该设备提供与其位置相关的信息检索或其他基础服务,比如搜索附近的餐厅,查询去往目的地的路线、时间等等,这大大便利了人们的生活.但是,基于位置的服务在方便人们生活的同时,也更容易暴露用户的位置隐私[2].一旦用户的位置隐私暴露,攻击者可以通过用户位置信息进行分析,直接或间接得到一些用户的其他隐私,比如用户的职业、身体状态(如生病去医院)等,攻击者还可以通过用户的位置信息,对用户进行追踪监控,这些都不是用户愿意接受的.并且随着用户对位置隐私保护意识的增强,用户开始倾向于不暴露自己精确的位置信息,而是只提供模糊的位置信息,这大大限制了位置相关应用的发展.因此,无论从用户角度来讲还是服务商角度来讲都需要位置隐私保护方案.如何在保证位置服务可用的基础上保护用户的位置隐私已成为一个越来越流行的话题.

网络安全领域,隐私一般指的是用户的身份信息.在分布式系统中,Wang等人[3]通过对2个最重要的匿名双因素方案进行密码分析作为案例研究,系统探讨了匿名双因素认证方案设计标准之间的内在冲突和不可避免的权衡,为在可用性、安全性和隐私性之间提供可接受的权衡做出了巨大贡献.在面向多网关的无线传感器网络多因素认证协议上,王晨宇等人[4]提出一个安全增强的可实现前向安全性的认证协议,在提高安全性的同时,保持了较高的效率,适于资源受限的无线传感器网络环境.这2个领域中,用户的身份信息都是需要被保护的,因为用户信息的暴露会带来一系列的其他隐私问题,如果登录用户身份泄露,攻击者会利用用户身份,对用户的活动进行跟踪,进行得到用户的敏感信息,比如年龄、性别、当前位置等.

在本文中,我们着重于位置隐私,将注意力放在用户具体的位置信息上.

在隐私保护方面,近年来差分隐私[5]在统计数据库等领域的隐私保护方面得到了广泛应用.差分隐私的目标是在进行统计查询时保护个人隐私,要求攻击者无法根据查询的结果推测出某个具体用户的信息[6-7].虽然差分隐私能够量化评估风险,但是仍存在着几个问题,首先是差分隐私在不同的场合往往需要具体定义,而具体的实现往往也有多种算法,不同定义之间、不同算法之间的安全程度缺乏统一的评估标准;其次,差分隐私在各种应用场景中,通常基于一些理想的统计模型,对于数据间本身具有的复杂关联关系考虑不足.

目前,已经有很多研究人员在基于位置的服务(location based service, LBS)上研究位置隐私,并提出了一系列位置隐私保护方案[8-17].根据隐私保护方案的使用场景,我们将其分为3类:位置点的位置隐私保护、轨迹的位置隐私保护,以及他们之上的位置集合隐私保护.轨迹是更偏向于时间序列方面的隐私保护,尽管有一些模型已考虑了相邻轨迹点间的关联关系,但是现有的隐私保护方案都未考虑整条轨迹对某一轨迹点的影响,即未考虑轨迹点间复杂的关联关系.此外,也缺少一种统一的对攻击算法定量的评估策略,虽然差分隐私希望通过概率的

方式来量化隐私的度量,但是它难以在不同的定义、不同的算法间客观地描述隐私保护程度.

为了客观地描述位置隐私的保护程度,本文针对轨迹的位置隐私保护,设计了利用简单关联关系的 Markov 攻击算法和利用复杂关联关系的深度神经网络攻击算法,并提出了一个可以定量评估攻击算法的方案,用于衡量脱敏轨迹的破解风险,即原轨迹经过位置隐私保护方案扰动后轨迹的破解风险.最后对基于差分隐私的 Geo-Indistinguishability[8] 隐私保护方案进行了攻击,并用本文所提出的评估方案对这 2 类攻击算法进行了量化评估,评估结果表明,能够利用复杂关联关系的深度神经网络算法具有更好的攻击效果.

本文的贡献有 3 个方面:

1) 设计了 Markov 攻击算法和深度神经网络攻击算法.Markov 攻击算法只考虑轨迹最近几个点对预测点的关联关系,是简单关联关系的代表,而深度神经网络攻击算法考虑了整条轨迹对预测点的关联关系,是复杂关联关系的代表.

2) 建立了一个定量的位置隐私攻击算法评估方案,用于衡量脱敏轨迹的破解风险.具体地,我们定义隐私数据距离函数,分别得到隐私保护方案脱敏轨迹和原轨迹的隐私数据距离与攻击算法预测轨迹和原轨迹的隐私数据距离,并将这 2 个距离的比较作为脱敏轨迹的破解风险.

3) 对 Geo-Indistinguishability 隐私保护方案进行攻击实验,使用 2 类攻击算法对其产生的脱敏轨迹进行攻击,并使用评估方案对 2 类攻击算法进行评估,结果表明 Geo-Indistinguishability 隐私保护方案抵御了 Markov 攻击算法的攻击,但未能抵御深度神经网络攻击算法的攻击.

1 背景和相关工作

目前,已经有很多研究人员针对位置隐私保护进行了研究,并提出了各类隐私保护方案.

根据位置隐私保护方案的使用场景,位置隐私保护分为位置集合场景下的隐私保护和位置点或者轨迹的位置隐私保护.首先介绍位置集合场景下的隐私保护,该场景主要是用于数据分析领域,即只需要提供一个脱敏后的位置轨迹集用于数据分析,不需要将每一条真实轨迹转化为一条脱敏轨迹.

Gursoy 等人[9]认为点的位置扰动容易受到推理攻击并且遭受严重的效用损失,因为它忽略了完整位置轨迹中的移动轨迹和连续性,并提出了 AdaTrace,这是一种可扩展的位置轨迹合成器,通过 4 个阶段:特征提取、概要学习、隐私和实用程序保留噪声注入以及差分隐私合成位置轨迹的生成来合成轨迹,并针对贝叶斯推理攻击、部分嗅探攻击和异常值泄露攻击对合成轨迹进行了过滤.

Bindschaedler 等人[10]将位置点语义信息加入到隐私保护方案里,其通过真实的位置和语义特征来设计的一种合成合理位置轨迹的系统方法,即生成地理位置虚假但语义真实的隐私保护位置轨迹,其中地理特征主要针对每个人(例如,每个人所指的"她的家"位于地理上不同的地方),而语义特征通常是通用的并且代表整体人类移动行为(例如,大多数人具有工作地点),并针对 2 类隐私威胁进行过滤.

接下来是位置点的位置隐私保护和轨迹的位置隐私保护,这 2 类隐私保护方案输入为一条轨迹或一个位置点,输出也是对应的脱敏轨迹或脱敏位置点.根据隐私保护方案使用的方法可分为 k-匿名法、假轨迹法和扰动法.k-匿名[11]法实现简单,计算量小,但是有一个很明显的缺点是无法保证攻击者知道辅助信息的数量,只有清楚了攻击者对辅助信息的了解情况,才可以用其他或虚拟的用户位置来迷惑攻击者.假轨迹法通常是用于轨迹集的数据发布,通过真实的轨迹集合来合成虚拟的轨迹,该方法实现较为简单,但可用性方面很难得到保障,丢失信息严重.扰动法是对轨迹点加入特定分布噪音的一种方法,具有隐私保护程度高,数据更真实的优点,但是在具有复杂时间序列的轨迹扰动场景下,由于现有的扰动类隐私保护模型很难考虑超出 Markov 的复杂关联性,因此其脱敏轨迹容易被利用轨迹间关系的攻击算法破解.

Gruteser 等人[11]最早将 k-匿名引入了位置隐私保护领域,这类方法中有些隐私方案要求攻击者无法推断出 k 个不同用户中是哪一个用户在进行查询.k-匿名一般是使用一个可信的第三方服务器来保护用户的位置[12-13],这种方式是要求 k 个轨迹点或 k 条轨迹不可分,常用的方法是将其他 $k-1$ 个用户的位置或者新生成 $k-1$ 个虚拟用户的位置一起发送进行查询,最后从查询结果中取出正确答案.

除了 k-匿名,也有很多直接对用户位置数据进行扰动的方法.

Geo-Indistinguishability 隐私保护方案由 Bordenabe 等人[8,14]基于差分隐私的思想提出,是属于位置点的隐私保护方案,差分隐私概念表达了

用户在使用基于位置的系统时的预期隐私要求,即可以保护用户的确切位置,同时仍然允许发布近似信息(通常需要获得某种所需服务),另外用极坐标下的拉普拉斯机制来实现.之后他们还将其转化为一个最优化问题,并提出了一个近似解决方案,大大降低了时间复杂度,但其并未考虑轨迹间的高相关性而针对此威胁进行防御.

Xiao 等人[15]结合用户位置之间的时间相关性运用 Markov 基于差分隐私的思想提出一种基于差异隐私的新定义"δ 位置集",以解释位置数据中的时间相关性,证明了众所周知的 L1 范数灵敏度未能捕捉到多维空间中的几何灵敏度,并提出了一个新概念灵敏度包,进而提出了一种用于位置扰动的平面各向同性机制(planar isotropic mechanism, PIM),PIM 是实现差分隐私下限的一种机制,最后通过实验证明了 PIM 保留了基于位置的查询的位置效用,并且显著优于基线拉普拉斯机制(laplace mechanism, LM).虽然该隐私保护方案考虑了轨迹相邻点之间的相关性,但由于轨迹中每个点之间都可能存在着相关的联系,因此该方案仍会被利用复杂关联关系的攻击算法威胁.

最后是隐私攻击方面的研究,在对隐私攻击进行评估前,需要先建立一个安全模型,用于明确隐私攻击方案要实现什么样的目标.如果不建立安全模型,很容易陷入"break-fix-break-fix"模式.多服务器环境下,汪定等人[18]通过对多个协议进行分析,将破坏前向安全性的攻击场景进行分类,突出被长期忽视的用户端口令泄露所引起的前向安全性问题以及智能卡安全参数泄露引起的前向安全性问题.在基于智能卡的密码认证方面,汪定等人[19]定义了一个安全模型,用于准确评估攻击者的实际能力,提出了一个评估认证方案的系统框架,为评估双因素身份验证方案提供了基准.遗憾的是,在位置隐私攻击的评估方面,还未见有人进行设计.

在位置隐私攻击方面,Rahman 等人[20]描述了一种针对成员攻击的攻击算法,通过 Shadow 模型来近似模拟云端的隐私保护方案,并通过 Shadow 模型得到攻击算法的训练集.具体而言,训练集的特征是 Shadow 模型的输出,如果数据来源于训练集,则标签为'in',表示目标模型用该数据训练过,否则标签为'out'.最后再通过一些深度模型进行攻击.

针对扰动法的隐私保护方案,虽然有人指出当前位置隐私模型未考虑轨迹点间存在的复杂关系[15],但并没有据此进行攻击.因此本文针对具有复杂时间序列的轨迹扰动场景进行了攻击,具体地,我们设计了利用简单关联关系的 Markov 攻击算法和利用复杂关联关系的深度攻击算法,并建立了一个定量的位置隐私攻击算法评估方案,用于衡量脱敏轨迹的破解风险.最后以 Geo-Indistinguishability 隐私保护方案为例进行实验,使用 2 类攻击算法进行攻击后,再使用评估方案对这 2 类攻击算法进行评估.

2 位置隐私攻击算法及评估方案

本节先对位置扰动的隐私保护方案和攻击算法所用的符号进行阐述;然后介绍利用简单关联关系的 Markov 攻击算法和利用复杂关联关系的深度神经网络攻击算法;最后提出了一个定量的评估方案,用于评估攻击算法对隐私保护方案的威胁程度.

2.1 隐私保护方案和攻击算法的符号定义

我们将用户的轨迹用张量 $\boldsymbol{V}$ 表示,用户的位置信息以用户 u 和用户轨迹 $\boldsymbol{V}$ 的 2 元组表示,对于第 k 组数据,可以用 $O^{(k)}=(u^{(k)},\boldsymbol{V}^{(k)})$ 表示,其中 $u^{(k)}$ 代表第 k 组数据中的用户,$\boldsymbol{V}^{(k)}$ 是第 k 组数据中的轨迹.用户和位置信息的数据集为

$$O_{\text{data}}=\{O^{(1)},O^{(2)},\cdots,O^{(n)}\}.$$

隐私保护方案是为了保护用户的隐私,其一般是通过对用户 u 进行匿名化处理或者对用户位置信息进行扰动实现,具体而言,我们可以用机制 $M=(A_u,A_v)$ 来代表一个隐私保护方案,其中 A_u 是原用户到脱敏数据用户的映射,A_v 是原用户轨迹到脱敏数据用户轨迹的映射.

原轨迹集 O_{data} 经过隐私保护方案后,得到脱敏数据 T_{data},对于扰动性查询的隐私保护方案,我们把经过隐私保护方案后的数据表示为

$$T_{\text{data}}=\{T^{(1)},T^{(2)},\cdots,T^{(n)}\}.$$

由于目前大部分隐私保护方案是只关注位置信息,因此,特别的,对于只关注位置信息的隐私保护方案,其输出为

$$T_{\text{data}}=\{A_v(\boldsymbol{V}^{(1)}),A_v(\boldsymbol{V}^{(2)}),\cdots,A_v(\boldsymbol{V}^{(n)})\}.$$

接下来是位置隐私攻击算法,我们假设攻击者可以上传真实轨迹给位置隐私保护方案,从而得到对应的脱敏轨迹.攻击者将对应的真实-脱敏轨迹对 $\langle O_k,T_k\rangle$ 作为训练集,构建一个从脱敏轨迹到真实轨迹的预测算法,因此攻击算法的输入数据即为隐私保护方案的输出数据.

攻击算法是为了得到更多的用户隐私,我们可以

用 $M'=(A'_u,A'_v)$来代表一个攻击算法,其中 A'_u 是脱敏数据用户到预测数据用户的映射,A'_v 是对脱敏数据用户轨迹到预测数据用户轨迹的映射.我们把经过攻击算法后的数据表示为

$$Pre_{\text{data}}=\{Pre^{(1)},Pre^{(2)},\cdots,Pre^{(n)}\}.$$

对于只关注位置信息的隐私保护方案,当脱敏轨迹经过攻击算法后,得到对原轨迹的预测轨迹为

$$Pre_{\text{data}}=\{A'_v(T^{(1)}),A'_v(T^{(2)}),\cdots,A'_v(T^{(n)})\}.$$

2.2 攻击算法

1 条轨迹含有多个轨迹点,这几个轨迹点有着极高的时间相关性和空间相关性.一般的隐私保护方案未考虑或未完全考虑这 2 个相关性,因此我们利用这 2 个相关性对隐私保护方案进行攻击,得到用户更为精准的位置轨迹或用户的其他信息.

下面先介绍利用简单关联关系的 Markov 攻击算法,之后再介绍攻击性更强利用复杂关联关系的深度神经网络攻击算法.

2.2.1 Markov 攻击算法

Markov 攻击算法是利用轨迹点间简单关联关系去攻击隐私保护方案的代表,首先我们需要定义几个基本的概念.

1) 释放概率[15]

原位置为 s_i,则输出脱敏位置为 s_j 的概率为

$$P(T_t=s_j\,|\,O_t=s_i).$$

2) 转移概率

时刻 t 的原位置为 s_i,则时刻 $t+1$ 的原位置为 s_j 的概率为

$$P(O_{t+1}=s_j\,|\,O_t=s_i).$$

释放概率和转移概率在预测轨迹时是作为先验知识,在训练集中计算得到转移矩阵 $\boldsymbol{M}$ 和释放矩阵 $\boldsymbol{R}$,释放概率和转移概率相互独立,进而可以求得预测轨迹时每次下一个位置的概率分布.具体地,时刻 t 预测位置为 a,在时刻 $t+1$ 脱敏位置为 b 的情况下,预测位置为 c 的概率为

$$P(O_{t+1}=c\,|\,O_t=a,T_{t+1}=b)=\frac{P(O_{t+1}=c,T_{t+1}=b\,|\,O_t=a)}{P(T_{t+1}=b\,|\,O_t=a)}=$$
$$\frac{P(O_{t+1}=c\,|\,O_t=a)P(T_{t+1}=b\,|\,O_{t+1}=c,O_t=a)}{\sum\limits_{k\in S}P(O_{t+1}=k\,|\,O_t=a)P(T_{t+1}=b\,|\,O_{t+1}=k,O_t=a)}=$$
$$\frac{P(O_{t+1}=c\,|\,O_t=a)P(T_{t+1}=b\,|\,O_{t+1}=c)}{\sum\limits_{k\in S}P(O_{t+1}=k\,|\,O_t=a)P(T_{t+1}=b\,|\,O_{t+1}=k)}.$$

由上,我们可以求得每次下一个位置的概率分布,并以此来生成脱敏轨迹.

轨迹的生成方案介绍如下.

1) 贪婪生成方案.隐私保护方案转换的脱敏位置为 f_k,当上一时刻预测的真实位置为 s^*_{k-1} 时,对于每一个位置 $s_k\in S$,S 为所有可能的位置集合,取 $P(O_{t+1}=s_k\,|\,O_t=s^*_{k-1},T_{t+1}=f_k)$ 最大的位置作为该时刻的预测位置,即

$$s^*_k=\max_{s_k\in S}P(O_{t+1}=s_k\,|\,O_t=s^*_{k-1},T_{t+1}=f_k).$$

2) Beam search 方案.按照贪婪生成方案,可以通过隐私化后的脱敏轨迹生成一条预测轨迹,这是对原轨迹即真实轨迹的预测.但是这样生成的轨迹只能保证局部最优.如果要保证全局最优,就只能枚举所有可能的轨迹,计算的时间复杂度高,开销大.因此我们选择了 2 种方案的折中,即 Beam search,这种方案有一个超参数 k.最开始的时候,我们选择当前时间条件概率最大的 k 个轨迹点,分布组成 k 条候选轨迹,接下来的一个时间步,对每一条候选轨迹进行穷举 1 步,假设轨迹点集合的大小为 L,我们将得到 $k\times L$ 条轨迹和对应的概率.取概率最大的 k 条轨迹,作为新的候选轨迹,为下一个时间步的生成做准备.如此循环,直到最后一个时间步,最后一个时间步概率最大的那条轨迹就是我们所预测的轨迹.

2.2.2 深度神经网络攻击算法

深度神经网络(deep neural network, DNN)是具有很多隐藏层的神经网络,在机器学习和人工智能的各种任务(例如图像分类、语音识别、机器翻译和游戏)中取得了巨大的成果.

在自然语言生成领域,大部分会用到 Seq2Seq 模型,Seq2Seq 模型一般是由 encoder 和 decoder 这 2 部分组成,而本文的位置隐私攻击算法正是属于其中的一种,但是不同的是,该模型的输入序列到输出序列是一个去噪音的过程,并且序列中每个点对预测点位置的影响和序列位置的距离有关,一般距离越近,影响越大.

循环神经网络(recurrent neural network, RNN)是一类具有短期记忆功能的深度神经网络,它不仅接收其他神经元的传递信息,还接收自身的信息,现已被广泛用于自然语言生成、语音识别等领域.RNN

非常适合在一些 Seq2Seq 的问题上使用,但是由于循环神经网络的参数更新是通过随时间的反向传播算法来学习的,因此当序列比较长的时候,会出现梯度消失或梯度爆炸[21]一些问题,这会导致循环神经网络的参数无法进行正确更新,从而导致循环神经网络无法学习到相隔较长的依赖问题,这也被称为长程依赖问题,为了解决长程依赖问题.有很多研究者对其进行了研究,其中有一种方式是引入门控机制,LSTM 就是其中很有效的一个模型.

LSTM[22]是循环神经网络的一个变体.其相比较于基础的循环神经网络,主要改进在 2 个方面:1)引入了新的内部状态 c,基础的 RNN 模块只有一个外部状态 h 代表着短期记忆,而 LSTM 引入了新的内部状态 c 来代表长期记忆;2)引入了门控机制,即通过精心设计的门来去除或增加信息到细胞状态.具体地,LSTM 使用遗忘门 f 来控制上一个时刻内部状态 c 需要遗忘多少信息,使用输入门 i 控制什么样的新信息需要添加到内部状态 c,使用输出门 o 控制当前时刻的内部状态 c 有多少信息需要输出.

另外还有 LSTM 的变体,比如双向长短记忆网络(bi-directional long short-term memory, Bi-LSTM)[23]等.LSTM 主要考虑上文的信息,而 Bi-LSTM 将下文的信息也添加到了内部状态.类似的 GRU 也是循环神经网络的一个变体,相比于 LSTM,它将遗忘门和输入门合并为一个单一的更新门,并混合了细胞状态的隐藏状态,最终的模型比标准的 LSTM 模型要简单,具有收敛更快,减少训练成本的效果,RNN 类攻击算法的模型结构图如图 1 所示.LSTM,GRU 也是类似,将 RNN 改为相应的结构即可,Bi-LSTM, Bi-GRU 则是增加一层反向的 RNN 结构.

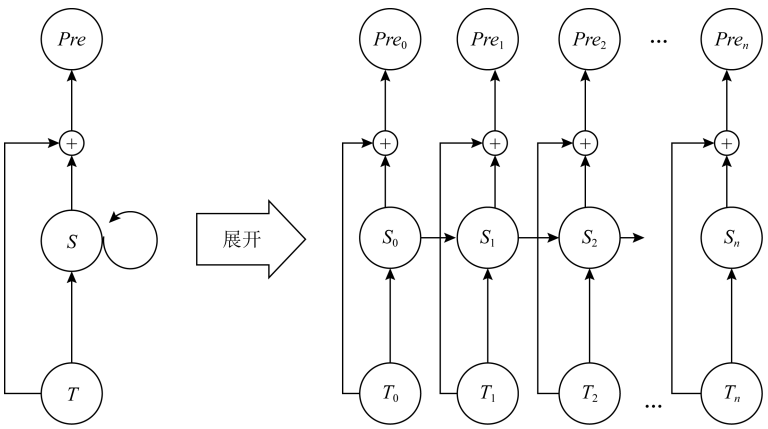


Fig. 1 Model structure diagram of RNN and residual network

图 1 RNN 和残差网络的模型结构图

本文依次用 LSTM,Bi-LSTM,GRU,Bi-GRU 攻击算法对测试模型进行攻击,攻击算法将 RNN 类模型结构和残差网络的模型结构结合.

2.3 攻击算法评估方案

首先我们需要定义数据间的一些距离度量函数.定义 d_{pri} 为和隐私相关数据的数据距离函数,它可以是任意的一个度量函数,输入是 2 条轨迹,输出是 1 个标量,代表着 2 条轨迹的数据距离,这里的映射方式可以自定义,比如可以用欧几里得距离的均值,或者搬土距离[24]等.在隐私保护方案场景下主要是针对隐私的综合考虑,其值越大表明隐私暴露越少,越小则隐私暴露越多.

我们用脱敏轨迹和原轨迹的隐私数据距离 $d_M^{(k)}=d_{\text{pri}}(O^{(k)},T^{(k)})$ 表示隐私保护方案 M 在第 k 个数据上对隐私的保护程度的估值,隐私保护方案对数据隐私保护程度越好,该值越大.另外,隐私保护方案对隐私的保护程度和泄露用户隐私的相关数据高度关联,例如如果用户位置隐私数据都在 x 轴时,假设单一位置是在一个 x,y 平面轴上,那么位置点和偏移后的位置点在 x 轴上的距离越大表明隐私保护效果越好,此时 $d_M^{(k)}$ 也越大.

$O_{\text{data}},T_{\text{data}}$ 中对应轨迹之间的隐私数据距离集合用 $D_{\text{pri}}(O_{\text{data}},T_{\text{dat}a})$ 表示:

$$D_{\text{pri}}(O_{\text{data}},T_{\text{data}})=\{d_M^{(1)},d_M^{(2)},\cdots d_M^{(n)}\}.$$

同样地,我们用预测轨迹和原轨迹的隐私数据距离 $d_{M'}^{(k)}=D_{\text{pri}}(O^{(k)},Pre^{(k)})$ 表示攻击算法 M' 对第 k 条脱敏轨迹威胁程度的估值.$O_{\text{data}},Pre_{\text{data}}$ 对应轨迹之间的隐私数据距离集合用 $D_{\text{pri}}(O_{\text{data}},Pre_{\text{data}})$ 表示:

$$D_{\text{pri}}(O_{\text{data}},Pre_{\text{data}})=\{d_{M'}^{(1)},d_{M'}^{(2)},\cdots,d_{M'}^{(n)}\}.$$

脱敏轨迹的破解风险,即攻击算法 M' 攻破隐私保护方案 M 的程度则是由 $D_{\text{pri}}(O_{\text{data}}, Pre_{\text{data}})$, $D_{\text{pri}}(O_{\text{data}}, T_{\text{data}})$ 计算比较得到.我们定义 2 个数据距离的比较函数 C,第 k 个数据上攻击算法攻破隐私的能力由 $C(d_M^{(k)}, d_{M'}^{(k)})$ 近似估计.比较函数 C 可以进行自定义,比如,我们可以简单地假设 $c^{(k)} = C(d_M^{(k)}, d_{M'}^{(k)}) = d_{M'}^{(k)}/d_M^{(k)}$.显然,$c^{(k)}$ 越小,则表明攻击算法 M' 在第 k 个数据上攻击得越成功,因此,我们把 $c^{(k)}$ 称为隐私保护方案 M 对攻击算法 M' 在第 k 个数据上的防御指数.

最后对攻击成功进行显式的定义,攻击成功需满足条件:

$$P_{M,M'} = \frac{1}{n}\sum_{k=1}^{n} 1(c^{(k)} < th_c) \geqslant th_{\text{pr}},$$

其中 $1(cond)$ 为 0-1 函数,当 $cond$ 为真时,该函数输出为 1,否则输出为 0,th_c 为防御指数的阈值,我们认为防御指数小于 th_c 时脱敏轨迹被破解,而 th_{pr} 为概率阈值,n 为数据的个数,$P_{M,M'}$ 是脱敏数据被破解的概率的估计值.

图 2 为隐私保护方案、攻击算法及评估攻击算法的流程图,其中①②是隐私保护方案,③④是攻击算法,⑤⑥是对攻击算法的评估.

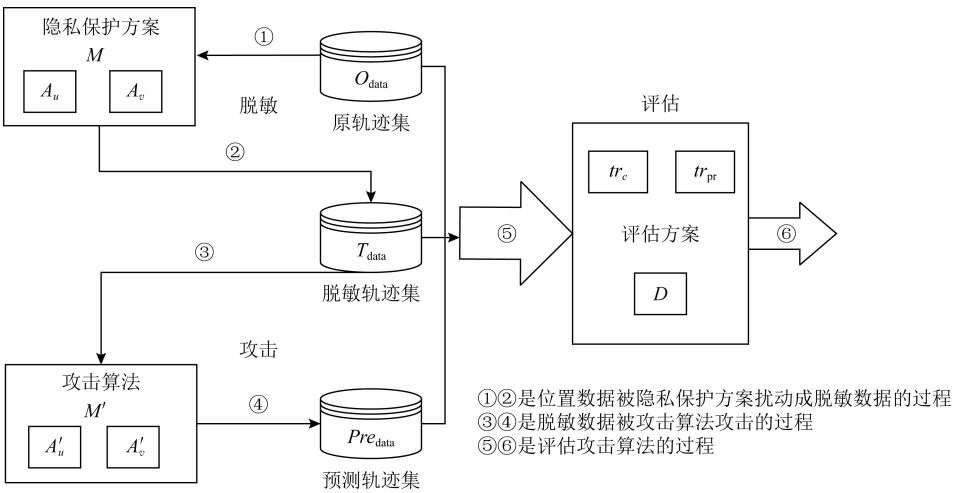


Fig. 2 Flow chart of location privacy algorithm

图 2 位置隐私算法流程图

3 对 Geo-Indistinguishability 的攻击

Geo-Indistinguishability 隐私保护方案在位置隐私领域是一个具有代表性的模型,该隐私保护方案被其他研究者广泛使用和比较[8,14-15,25-26].本节将阐述 Geo-Indistinguishability 隐私保护方案,并介绍使用 2 类攻击算法对其进行攻击后,如何使用攻击算法的评估方案对这 2 类攻击算法进行评估.

3.1 Geo-Indistinguishability

Geo-Indistinguishability 的核心思想是任 2 个距离小于等于 r 的点 x, x',各自加入扰动后生成的点在点集 S 上的概率比不超过 $e^{\varepsilon d(x,x')}$,令 Z 为所有位置点的集合,则公式定义为

$$P(S|x) \leqslant e^{\varepsilon d(x,x')} P(S|x'), \forall x, x' \in X, \forall S \subseteq Z.$$

文献[8]是通过加入拉普拉斯噪声来实现的,即加入偏移量的概率分布为

$$D_\varepsilon(x_0)(x) = \varepsilon^2 e^{-\varepsilon d(x_0,x)}/2\pi.$$

将以上概率分布转化为极坐标下的拉普拉斯噪声,可得

$$D_\varepsilon(r,\theta) = \frac{\varepsilon^2}{2\pi} r e^{-\varepsilon r}.$$

计算 D 关于 r, θ 的边缘分布,得到

$$D_\varepsilon(r,\theta) = D_{\varepsilon,R}(r) D_{\varepsilon,\Theta}(\theta),$$

其中

$$D_{\varepsilon,R}(r) = \varepsilon^2 r e^{-\varepsilon r}, D_{\varepsilon,\Theta}(\theta) = \frac{1}{2\pi}.$$

本文通过采样 r 和 θ 来实现 Geo-Indistinguishability 机制.

对于 r,我们令 $C_\varepsilon(r)$ 代表隐私化后位置到原位置距离小于 r 时的概率,即

$$C_\varepsilon(r) = \int_0^r \varepsilon^2 \rho e^{-\varepsilon\rho} d\rho = 1 - (1+\varepsilon r) e^{-\varepsilon r}.$$

因此只需要从[0,1)的均匀分布中采样 p,然后通过计算 $r = C_\varepsilon^{-1}(p)$,就可以得到符合拉普拉斯噪声分布的 r.

对于 θ,θ 直接从[0,2π)均匀分布中直接采样得到即可.

当用户的轨迹由多个轨迹点组成时,Geo-Indistinguishability 对每一个轨迹点都进行一次独立的扰动,每次扰动都未考虑轨迹点间很强的关联关系,因此,可以利用这些关联关系对其进行攻击.

3.2 评估方案

由于采样 r 时是先从[0,1)的均匀分布中采样 p,然后通过计算得到,因此为方便评估,我们将 L_2 距离 r 转换为 p 距离.具体地,对于原轨迹点和对应的脱敏轨迹点的 L_2 距离 r,通过 $p=C_\varepsilon(r)$ 得到 p 距离.显然 r 是 p 的递增函数,p 越小,偏移的距离越小.另外,由于隐私保护模型中,p 是从[0,1)均匀分布中采样得到,那么轨迹脱敏后,脱敏轨迹点和原轨迹点的 p 距离应有 20%落在 0~0.2 上,40%落在 0~0.4 上.但是由于轨迹所选活动区域受限,故在进行隐私处理时进行了截断处理,当 ε 很小的时候,大部分点都进行了截断,导致原轨迹-隐私化后轨迹的 p 距离不在[0,1]均匀分布,因此需要对原轨迹-隐私化后轨迹和原轨迹-预测轨迹进行比较才合适.

对于任意 1 组原轨迹、脱敏轨迹、预测轨迹,我们可以计算出原轨迹和脱敏轨迹对应点间的 p 距离,进而可得到 2 条轨迹的 p 距离分布.同样地,我们也可得到原轨迹和预测轨迹的 p 距离分布,通过比较这 2 个 p 距离分布来评估攻击算法攻破 Geo-Indistinguishability 的程度.

在攻击算法的评估中,令隐私相关数据的数据距离函数 d_{pri} 为轨迹中每一点转为 p 距离后的均值,即 $d_{\text{pri}}(O^{(k)},T^{(k)})=\sum_{i=1}^{m}p(T^{(k)i},O^{(k)i})/m$,其中 p 为将脱敏轨迹点转换为 p 距离的映射,m 为轨迹中轨迹点的个数,2 个数据距离的比较函数 $c^{(k)}=C(d_M^{(k)},d_{M'}^{(k)})=d_{M'}^{(k)}/d_M^{(k)}$,即预测轨迹和原轨迹的轨迹距离比上脱敏轨迹和原轨迹的轨迹距离,显然这个比值越小,说明攻击算法攻击得越成功.

4 实 验

4.1 数据集

本文使用了 Geolife[27] 数据.此数据来自于微软的 GeoLift 项目,该项目从 2007 年 4 月到 2012 年 8 月收集了 182 个用户的轨迹数据,还记录了一系列用户的位置时间信息,包括纬度、经度和时间戳等,并且轨迹是高时间连续的,每 1~60 s 更新 1 次.在这个数据中,我们过滤北京三环外的数据,得到北京三环以内的所有轨迹作为我们的数据集,并按照 Geo-Indistinguishability 中描述的方法,将北京三环内的地图划分为 38×50 的区域块.将数据集转化为区域块号序列的轨迹集后,通过 Geo-Indistinguishability 隐私保护方案,对原轨迹进行脱敏处理,进而得到一一对应的脱敏轨迹,我们将其按 8∶2的比例分为训练集和测试集.

Markov 攻击算法将在训练集中得到包含所有转移概率的转移矩阵和包含所有释放概率的释放矩阵,之后在测试集中进行攻击.

深度神经网络攻击算法将把训练集中的脱敏轨迹作为输入,一一对应的原轨迹作为输出进行训练.在测试集中进行攻击时,将测试集中的脱敏轨迹作为输入,深度神经网络得到的结果即为预测轨迹.

4.2 实验设置

本文使用 Geo-Indistinguishability 隐私保护方案生成脱敏轨迹,并将数据集分为训练集 A 和测试集 T,每一个数据包括原轨迹和对应的脱敏轨迹.之后分别使用 Markov 攻击算法和多个深度神经网络攻击算法对其进行攻击,并对各个攻击算法进行了评估.

在 Markov 攻击算法中,本文将活动区域划分为 38×50 的区域,并在训练集 A 中进行统计得到包含所有转移概率的转移矩阵和包含所有释放概率的释放矩阵,矩阵大小都有 1 900×1 900,然后在测试集中进行测试.本文使用 Beam search 的生成方式,并取 $k=10$,这样对测试集 T 每一条脱敏轨迹进行预测生成预测轨迹集.

在深度神经网络攻击算法中,LSTM,GRU,Bi-LSTM,Bi-GRU 攻击算法均使用 64 维隐藏变量,输入输出皆为位置的轨迹原始数据,即 $n\times2$ 的张量,其中 n 为轨迹中数据点的个数,输出也为 $n\times2$ 的张量,并在训练集中进行训练,损失函数为预测轨迹和真实轨迹的均方误差损失(MSE loss).训练时以 3E-4 的学习率,使用 Adam 优化器训练 100 轮.之后对测试集 T 每一条脱敏轨迹进行预测,生成预测轨迹集.

最后在攻击算法评估中,我们分别计算了 ε 在 0.1,0.3,0.5,0.7,1.1,1.5,2.1 的情况下 Geo-Indistinguishability 对 Markov 攻击算法和深度神经网络攻击算法防御指数的分布,本文中的 ε 都是指 Geo-Indistinguishability 公式定义中的 ε.

4.3 实验结果

本文分别使用 Markov 攻击算法和深度攻击算法对 Geo-Indistinguishability 隐私保护方案生成的脱敏轨迹进行攻击.

4.3.1 Markov 攻击算法结果

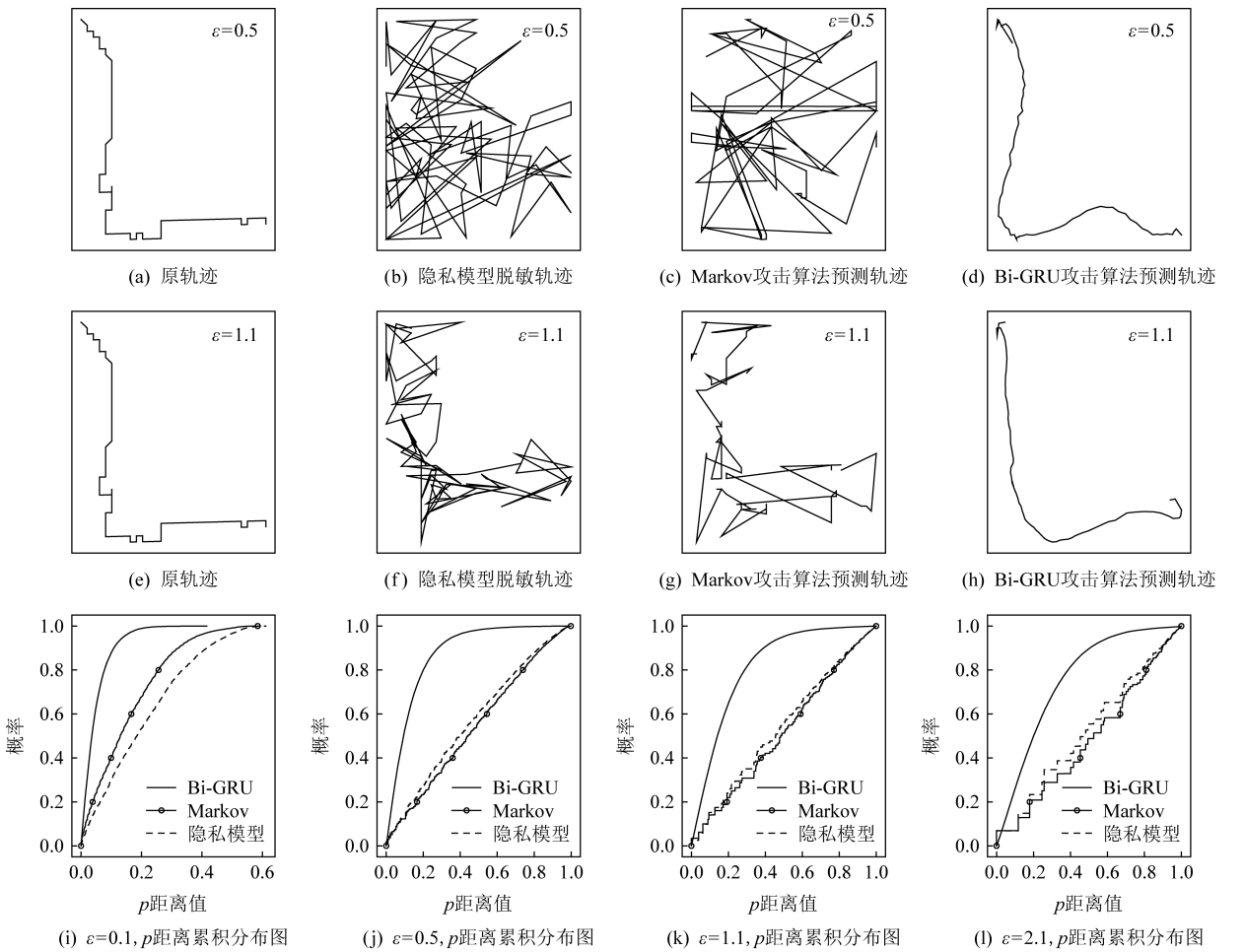
按照 2.2.2 节中所描述的方法,我们在训练集中得到包含所有转移概率的转移矩阵和包含所有释放概率的释放矩阵,然后在测试集中进行测试.我们使用取 $k=10$ 的 Beam search 的生成方式,对测试集每一条轨迹进行预测生成.实验结果如图 3(a)(b)(c)(e)(f)(g).

图 3 中,可以看出攻击算法预测轨迹和隐私保护方案脱敏轨迹相比,并没有和真实轨迹更加接近,主要的原因有 2 方面:1)Markov 攻击算法预测本次轨迹点时只考虑了上一个轨迹点的预测位置和本次脱敏轨迹点位置,这和现实中的模型不符,现实中的轨迹中任 2 个轨迹点都可能强相关;2)数据集中的数据不够多,导致我们所求的转移矩阵和释放矩阵都较为稀疏,不能很好地表示实际情况.另外从图 3(i)~(l)不同 ε 情况下的脱敏轨迹和 Markov 攻击算法预测轨迹的 p 距离的累积分布图可以看出,这 2 个 p 距离分布在 ε 较大时基本保持一致,而在 $\varepsilon=0.1$ 时,这 2 个 p 距离分布也只是轻微的不一致.即该攻击算法不能攻破 Geo-Indistinguishability 隐私保护方案的隐私.

4.3.2 深度神经网络攻击算法结果

按照 2.2.2 节中所描述的方法,我们在训练集中训练 Bi-GRU,GRU,Bi-LSTM,LSTM 攻击算法的参数,然后在测试集中进行测试,实验结果如图 3 和图 4 所示.

图 3(d)(h)为 Bi-GRU 在不同的 ε 下的预测轨迹,图 4(c)~(f)分别为 LSTM,GRU,Bi-LSTM,Bi-GRU 攻击算法的预测轨迹,可以看出攻击算法预测轨迹和隐私保护方案脱敏轨迹相比,攻击算法预测的轨迹明显和真实轨迹更像,也就是说该攻击算法很可能对隐私保护方案造成了很大的威胁.再由



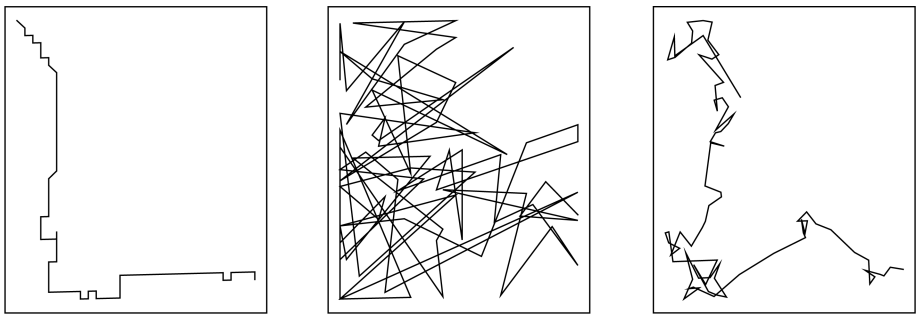
(a) 原轨迹 (b) 隐私模型脱敏轨迹 (c) Markov攻击算法预测轨迹 (d) Bi-GRU攻击算法预测轨迹

(e) 原轨迹 (f) 隐私模型脱敏轨迹 (g) Markov攻击算法预测轨迹 (h) Bi-GRU攻击算法预测轨迹

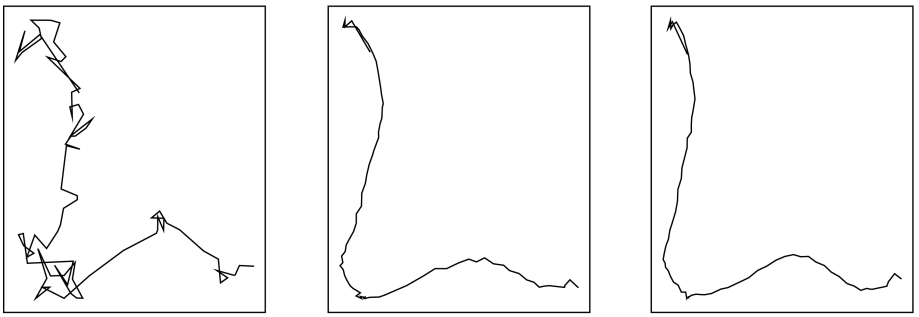
(i) $\varepsilon=0.1$, p距离累积分布图 (j) $\varepsilon=0.5$, p距离累积分布图 (k) $\varepsilon=1.1$, p距离累积分布图 (l) $\varepsilon=2.1$, p距离累积分布图

Fig. 3 Markov, Bi-GRU comparison graph

图 3 Markov,Bi-GRU 对比图



(a) 原轨迹 (b) 隐私模型脱敏轨迹 (c) LSTM攻击算法预测轨迹



(d) GRU攻击算法预测轨迹 (e) Bi-LSTM攻击算法预测轨迹 (f) Bi-GRU攻击算法预测轨迹

Fig. 4 Track comparison example($\varepsilon=0.5$)

图 4 轨迹对比示例($\varepsilon=0.5$)

图 3(i)～(l)可以看出 $\varepsilon=0.5,1.1,2.1$ 时,Bi-GRU 攻击算法得到的预测轨迹的 p 距离值小于 0.6 的轨迹概率都超过 80%,而隐私保护方案得到的 p 距离概率分布中小于 0.6 的轨迹概率都在 60%左右,$\varepsilon=0.5$ 时分布的差距更加大,Bi-GRU 攻击算法得到的预测轨迹的 p 距离值小于 0.6 的轨迹概率甚至超过了 95%,这里不对 $\varepsilon=0.1$ 的情况讨论,是因为此时,由于隐私保护方案加的噪音过大,导致很多轨迹点超出了规定的范围进行了截断处理,所以导致脱敏轨迹的 p 距离分布和 0-1 均匀分布有很大的差别.以上结果说明在该攻击算法攻击 Geo-Indistinguishability 的效果达到了预期,并且 ε 取值小时,攻击效果更佳.

4.3.3 攻击算法定量评估及实验结果分析

1) 深度攻击算法间的对比

由图 3 可以看出相比较于脱敏轨迹,Bi-GRU,GRU,Bi-LSTM,LSTM 攻击算法明显和原轨迹更接近,Bi-GRU 和 Bi-LSTM 的攻击效果比较接近,并且优于 GRU 和 LSTM 的攻击效果.图 5(c)可以看出,如果将防御指数阈值设置为 0.6,LSTM 和 GRU 有接近 80%的轨迹达到了预期,而 Bi-LSTM 和 Bi-GRU 超过 90%的轨迹达到了预期.Bi-LSTM 和 Bi-GRU 的效果更好的原因是轨迹中的点不仅和过去的轨迹点相关,还与未来的轨迹点相关,LSTM 或 GRU 攻击算法只考虑了过去的轨迹点,另外由于攻击算法进行攻击时得到的是整条脱敏轨迹,因此可以使用未来的脱敏轨迹点数据.

2) Markov 攻击算法和 Bi-GRU 攻击算法对比

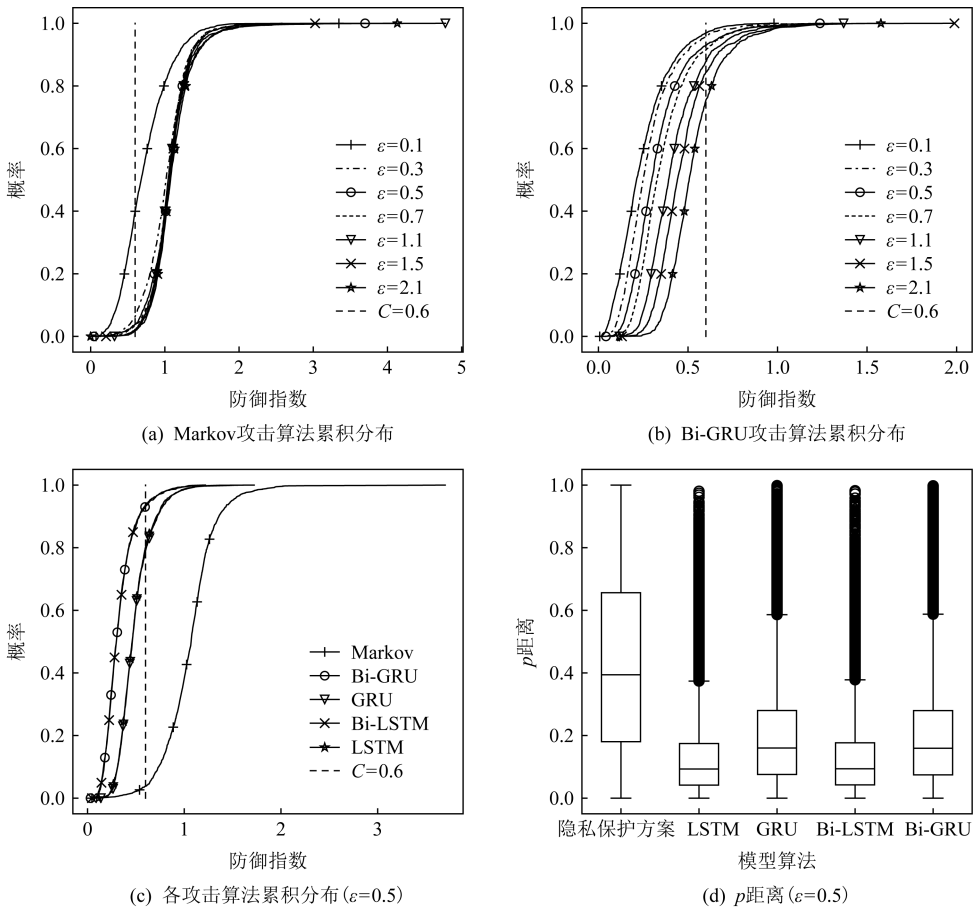
图 5 和表 1 是 Markov 攻击算法和 Bi-GRU 攻击算法在不同 ε 下得到的实验结果.

由图 5(a)(b)可以看出 Geo-Indistinguishability 抵挡住了 Markov 的攻击,但没有抵挡住深度神经网络的攻击,并且,由图 5(b),在一定范围内,隐私预算 ε 越小,Bi-GRU 攻击算法对 Geo-Indistinguishability 隐私保护方案的威胁越大.

由表 1,假定设置防御指数阈值为 0.6,Bi-GRU 攻击成功的轨迹比例随着 ε 的降低不断增加,ε 从 2.1 降到了 0.1,攻击成功的比例从 75%提高至 97%,出现这个情况的原因可能是当隐私预算很大时,轨迹点本来就偏离的不多,而当隐私预算小的时候,轨迹点偏离距离较大,攻击算法可以更好地利用轨迹点间的高相关性,去预测真实轨迹的位置.至于 Geo-Indistinguishability 隐私保护方案为什么在不同的 ε 中 p 距离概率分布不同的原因已在 3.2 节中进行了说明,主要是因为所选活动区域的限制,在进行隐私处理时进行了截断处理.

在攻击算法评估中,假如我们设定攻击成功中的概率阈值为 0.8,防御指数阈值为 0.6,那么 Geo-

Indistinguishability 完全抵御了 Markov 的攻击，而 Bi-GRU 在 ε=0.1,0.3,0.5,0.7,1.1,1.5 的情况下攻击达到了预期，可以看出在一定范围内，ε 越小，攻击越成功，主要原因是 ε 过大时，原轨迹只加了很小的扰动便得到了脱敏轨迹，脱敏轨迹和原轨迹间的数据距离本身就很小，从而导致了攻击算法失效.



(a) Markov攻击算法累积分布 (b) Bi-GRU攻击算法累积分布

(c) 各攻击算法累积分布(ε=0.5) (d) p距离(ε=0.5)

Fig. 5 Attack algorithm comparison graph

图 5 攻击算法对比图

Table 1 Comparison of Bi-GRU and Markov Attack Algorithm Results

表 1 Bi-GRU 和 Markov 攻击算法结果对比表

ε 取值	Bi-GRU 攻击算法		Markov 攻击算法	
	防御指数平均值	预测轨迹成功率	防御指数平均值	预测轨迹成功率
0.1	0.249	0.969	0.730	0.399
0.3	0.281	0.959	1.020	0.063
0.5	0.331	0.929	1.066 3	0.039
0.7	0.363	0.915	1.055	0.038
1.1	0.423	0.877	1.081	0.023
1.5	0.473	0.843	1.094	0.018
2.1	0.534	0.754	1.105	0.023

5 结论及展望

在本文中，我们提出了一个通用的针对位置信息扰动的隐私框架和攻击框架，并提出了一个定量评估攻击算法的策略.另外由于一条轨迹的轨迹点序列有着很强的相关性，而大部分隐私保护方案未考虑这种相关性或未完全考虑到这种相关性，我们认为很有可能通过轨迹点间的相关性获得用户位置隐私，因此我们分别使用 Markov 攻击算法和深度

神经网络攻击算法对 Geo-Indistinguishability 隐私保护方案进行了攻击,实验结果发现 Geo-Indistinguishability 能抵御 Markov 的攻击,但不能抵御深度神经网络攻击算法的攻击.

将来,一方面我们将设计更好的攻击算法,来提升攻击算法的攻击能力和泛化能力;另一方面,我们希望通过深度对抗的方式,生成一个能够抵御这类攻击的隐私保护方案.

作者贡献声明:沈钲晨是本研究的实验设计者和实验研究的执行人,完成数据分析,论文初稿的写作;张千里、王继龙是项目的构思者及负责人,张千里指导实验设计、数据分析、论文写作与修改;张超凡、唐翔宇参与实验设计和实验结果分析.

参 考 文 献

[1] Dey A, Hightower J, de Lara E, et al. Location-based services [J]. IEEE Pervasive Computing, 2010, 9(1): 11-12

[2] Beresford A, Stajano F. Location privacy in pervasive computing [J]. IEEE Pervasive Computing, 2003, 2(1): 46-55

[3] Wang Ding, He Debiao, Wang Ping. Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment [J]. IEEE Transactions on Dependable and Secure Computing, 2015, 12(4): 428-442

[4] Wang Chenyu, Wang Ding, Wang Feifei, et al. Multi-factor user authentication scheme for multi-gateway wireless sensor networks [J]. Chinese Journal of Computers, 2020, 43(4): 683-700 (in Chinese)
(王晨宇, 汪定, 王菲菲, 等. 面向多网关的无线传感器网络多因素认证协议[J]. 计算机学报, 2020, 43(4): 683-700)

[5] Dwork C, Roth A. The algorithmic foundations of differential privacy [J]. Foundations and Trends in Theoretical Computer Science, 2014, 9(3/4): 211-407

[6] Zhu Tianqing, Li Gang, Zhou Wanlei. Differentially private data publishing and analysis: A survey [J]. IEEE Transactions on Knowledge and Data Engineering, 2017, 29(8): 1619-1638

[7] Xiong Ping, Zhu Tianqing, Wang Xiaofeng. A survey on differential privacy and applications [J]. Chinese Journal of Computers, 2014, 37(1): 101-122 (in Chinese)
(熊平, 朱天清, 王晓峰. 差分隐私保护及其应用[J]. 计算机学报, 2014, 37(1): 101-122)

[8] Miguel A, Nicolás B, Kostas C, et al. Geo-Indistinguishability: Differential privacy for location-based systems [C] //Proc of the ACM Conf on Computer and Communications Security(CCS'13). New York: ACM, 2013: 901-914

[9] Gursoy M, Liu Ling, Truex S, et al. Utility-aware synthesis of differentially private and attack-resilient location traces [C] //Proc of the 2018 ACM SIGSAC Conf on Computer and Communications Security (CCS'18). New York: ACM, 2018: 196-211

[10] Bindschaedler V, Shokri R. Synthesizing plausible privacy-preserving location traces [C] //Proc of 2016 IEEE Symp on Security and Privacy (SP). Piscataway, NJ: IEEE, 2016: 546-563

[11] Gruteser M, Grunwald D. Anonymous usage of location-based services through spatial and temporal cloaking [C] //Proc of the 1st Int Conf on Mobile Systems, Applications and Services. New York: ACM, 2003: 31-42

[12] Zhang Chengyang, Huang Yan. Cloaking locations for anonymous location based services: A hybrid approach [J]. GeoInformatica, 2009, 13(2): 159-182

[13] Gkoulalas-Divanis A, Kalnis P, Verykios V. Providing k-anonymity in location based services [J]. SIGKDD Explorations, 2010, 12(1): 3-10

[14] Bordenabe N, Chatzikokolakis K, Palamidessi C. Optimal geo-indistinguishable mechanisms for location privacy [C] //Proc of the 2014 ACM SIGSAC Conf on Computer and Communications Security(CCS'14). New York: ACM, 2014: 251-262

[15] Xiao Yonghui, Xiong Li. Protecting locations with differential privacy under temporal correlations [C] //Proc of the 22nd ACM SIGSAC Conf on Computer and Communications Security(CCS'15). New York: ACM, 2015: 1298-1309

[16] Pan Xiao, Hao Xing, Meng Xiaofeng. Privacy preserving towards continuous query in location-based services [J]. Journal of Computer Research and Development, 2010, 47(1): 121-129 (in Chinese)
(潘晓, 郝兴, 孟小峰. 基于位置服务中的连续查询隐私保护研究[J]. 计算机研究与发展, 2010, 47(1): 121-129)

[17] Deng Miwen.Side information fusion dual anonymous location privacy protection scheme [J]. Journal of Information Security Research, 2020, 6(5): 421-426 (in Chinese)
(邓密文. 融合边信息的双重匿名位置隐私保护方案[J]. 信息安全研究, 2020, 6(5): 421-426)

[18] Wang Ding, Li Wenting, Wang Ping. Crytanalysis of three anonymous authentication schemes for multi-server environment [J]. Journal of Software, 2018, 29(7): 1937-1952 (in Chinese)
(汪定, 李文婷, 王平. 对三个多服务器环境下匿名认证协议的分析[J]. 软件学报, 2018, 29(7): 1937-1952)

[19] Wang Ding, Wang Ping. Two birds with one stone: Two-factor authentication with security beyond conventional bound [J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(4): 708-722

[20] Rahman M, Rahman T, Laganière R, et al. Membership inference attack against differentially private deep learning model [J]. Transactions on Data Privacy, 2018, 11(1): 61-79

[21] Informatik F, Bengio Y, Frasconi P, et al. A Field Guide to Dynamical Recurrent Neural Networks [M]. Piscataway, NJ: IEEE, 2001: 237-243

[22] Sak H, Senior A, Beaufays F. Long short-term memory based recurrent neural network architectures for large vocabulary speech recognition [J]. arXiv preprint, arXiv: 1402.1128, 2014

[23] Huang Zhiheng, Xu Wei, Yu Kai. Bidirectional LSTM-CRF models for sequence tagging [J]. arXiv preprint, arXiv: 1508.01991, 2015

[24] Rubner Y, Tomasi C, Guibas L. Metric for distributions with applications to image databases [C] //Proc of the 6th Int Conf on Computer Vision. Piscataway, NJ: IEEE, 1998: 59-66

[25] Krumm J. A survey of computational location privacy [J]. Personal and Ubiquitous Computing, 2009, 13(6): 391-399

[26] Butt T, Iqbal R, Salah K, et al. Privacy management in social internet of vehicles: Review, challenges and blockchain based solutions [J]. IEEE Access, 2019, 7: 79694-79713

[27] Zheng Yu, Xie Xing, Ma Weiying. Geolife: A collaborative social networking service among user, location and trajectory [J]. IEEE Data Engineering Bulletin, 2010, 33(2): 32-39

Shen Zhengchen, born in 1994. Master. His main research interest is location privacy.

沈钲晨,1994 年生.硕士.主要研究方向为位置隐私.

Zhang Qianli, born in 1975. PhD, associate professor. His main research interests include next generation Internet architecture, network security.

张千里,1975 年生.博士,副研究员.主要研究方向为下一代互联网架构、网络安全.

Zhang Chaofan, born in 1998. Master candidate. His main research interest is the application of SRv6.

张超凡,1998 年生.硕士研究生.主要研究方向为 SRv6 应用.

Tang Xiangyu, born in 1998. Master candidate. His main research interest is location network.

唐翔宇,1998 年生.硕士研究生.主要研究方向为位置网.

Wang Jilong, born in 1973. PhD, professor. His main research interests include next generation Internet architecture, network security, network measurement.

王继龙,1973 年生.博士,教授.主要研究方向为下一代互联网架构、网络安全、网络测量.