

Article

A Game-Theoretic Framework to Preserve Location Information Privacy in Location-Based Service Applications

Mulugeta Kassaw Tefera  and Xiaolong Yang *

School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China; mulugetaksw@gmail.com

* Correspondence: yangxl@ustb.edu.cn

Received: 27 January 2019; Accepted: 28 March 2019; Published: 1 April 2019



Abstract: Recently, the growing ubiquity of location-based service (LBS) technology has increased the likelihood of users' privacy breaches due to the exposure of their real-life information to untrusted third parties. Extensive use of such LBS applications allows untrusted third-party adversarial entities to collect large quantities of information regarding users' locations over time, along with their identities. Due to the high risk of private information leakage using resource-constrained smart mobile devices, most LBS users may not be adequately encouraged to access all LBS applications. In this paper, we study the use of game theory to protect users against private information leakage in LBSs due to malicious or selfish behavior of third-party observers. In this study, we model a scenario of privacy protection gameplay between a privacy protector and an outside visitor and then derive the situation of the prisoner's dilemma game to analyze the traditional privacy protection problems. Based on the analysis, we determine the corresponding benefits to both players using a point of view that allows the visitor to access a certain amount of information and denies further access to the user's private information when exposure of privacy is forthcoming. Our proposed model uses the collection of private information about historical access data and current LBS access scenario to effectively determine the probability that the visitor's access is an honest one. Moreover, we present the procedures involved in the privacy protection model and framework design, using game theory for decision-making. Finally, by employing a comparison analysis, we perform some experiments to assess the effectiveness and superiority of the proposed game-theoretic model over the traditional solutions.

Keywords: mobile networks; location-based service; security and privacy; game-theory; privacy preservation; prisoner's dilemma; Nash Equilibrium

1. Introduction

Location-based services (LBSs) are becoming increasingly popular, empowering ordinary mobile users with the capacity to access convenience services through wireless networks while, at the same time, sharing location information with possibly untrusted third-party adversarial entities using their Smartphone devices. The key idea behind LBS is to continuously access the users' private information attached to their locations and service attributes when they interact with such LBS applications. Despite the convenience of LBS applications, many privacy challenges still exist and affect LBS users in various ways. Therefore, existences of vulnerable mobile social network, the lack of users' awareness of their own privacy protection, and untrusted LBS providers have become the primary factors causing the leakage of users' personal interests, habits, relationships, and activities [1–4]. Even mobile users who may question LBS applications' results may disclose their real locations and potential interests

associated with LBSs [5]. According to a survey [6], with the development of mobile social networks and growing use of LBSs, 85% of Internet users are generally worried that their personal data will be acquired and spread by others, which poses a serious threat to personal privacy. There are two main reasons for the leakage of user privacy information in the network: technical defects and interest temptations. At present, researchers have proposed many solutions to protect users' location privacy, which mainly focused on preventing the leakage of users' private information through technical means or unwillingly exposing their location to adversarial third-party applications. Recent works [7–9] on location privacy have found that a visiting attacker can always access the target's location history and then launch attacks any time to disclose the correlation between the real identities of the users and their pseudonyms, even when a user's location information is obfuscated in the presence of location privacy-preserving mechanisms (LPPMs). Therefore, once the location information and user's identity attached to the LBS queries have been leaked through other techniques or side-channels, users have no means to control their private information, and all aspects of their personal privacy will be revealed.

To address this problem, a large number of privacy-enhancing mechanisms have been proposed to make use of LBSs, providing them to users, while limiting the amount of sensitive information leaked through observation [10–12]. These privacy-preserving mechanisms include location anonymization and user access control mechanisms that attempt to address location privacy issues in location and mobile social networks [13]. Location anonymization is one of the most widely used protection mechanism. It aims to use the anonymous information without using the user's real location information to obtain the private information of the users [14,15]. The most widely used mechanisms include location obfuscation or spatial-temporal cloaking techniques. However, the protection issue in the anonymization approach is not the possibility of the private information of the owner him/herself being revealed, but the real identity of the private information owner. Therefore, if the real identity information of the user has leaked through the use of LBSs, then all aspects of the user's privacy will be exposed. On the other hand, the privacy protection mechanism, based on an access control scenario, implements the protection technique from an internal perspective. This mechanism refers to the type of techniques used to appropriately extend the traditional information security-oriented access control mechanisms to achieve the requirements of mitigating various of users' private information leaking issues [16–18]. However, most of these protection mechanisms rely on different technical means in the prevention of the disclosure of a user's private information and thus has some advantages and disadvantages.

In this paper, we consider the growing use of LBSs to analyze the privacy protection effects from the behavioral interest and game-theoretic perspectives and demonstrate a privacy protection model to be used when third-party visitors access an LBS user's trajectory. We let the LBSs that enable their users to continuously access them and easily obtain their private information, leaked from their frequently visited routes. Considering the reality that mobile users may not be adequately inspired to access LBSs due to the high risk of privacy using resource-constrained mobile devices, we apply a game-theoretic privacy protection model to analyze the impact of user query behaviors, and identify the Nash equilibrium (NE) solutions. The systems outside the observer could access the user's trajectory in order to obtain his/her private information through the use of LBSs. When the visitor makes a request to access the user's private information, the user will decide whether to allow the access query, based on the privacy protection strategy. In this process, it is assumed that both the user and the outsider must pay a certain privacy cost for the possible actions, and the benefits obtained are the factors to be considered and measured in the process of making decisions. Here, we observe the following two important principles [19]: First, different users have different degrees of tolerance for the disclosure of their private sensitive data, reflecting their will to conceal their private information. Second, we suppose that the number of visits by the visitor to the same user has a superposition effect, i.e., as the number of visits to private information increases, the probability that the visitor acquires the user's private information will also increase and thus the awareness of the user to his/her private information disclosure and protection actions should also increase.

To analyze the privacy protection problem more effectively, this work is particularly remarkable, because it contains a classic game theory-based privacy protection model that makes it possible for the mobile user and the outside visitor (who aims to obtain the user's personal data) to compute the game strategies and their corresponding benefits. Based on the benefit, there may be NE in the gameplay between the two parties, and the probability of the visitor's good-faith access through the equilibrium solution. For this purpose, the user can set a threshold in the privacy protection strategy, according to his or her tolerance of private information leakage. We assume that the visitor is also knowledgeable of this setting of the threshold quality constraint. The game strategies, adopted by both the user and the outsider, can be implemented. From a gaming perspective, the protection model realizes the benefits from the point of view of good-faith or malicious access and allows access to a certain extent (i.e., private information leakage) or denies access (i.e., no leakage). Based on this, the game strategy that can be adopted by the LBS users is "allow access" or "deny access" to their private information, while the visitor adopts a "good-faith access" or "malicious access" strategy in the process of visiting the user's trajectory. Therefore, the visitor's access request to the user is allowed only when the probability of the visitor's good-faith access is higher than the threshold quality constraint. After each visit, the user records the access request involved in the visit as a factor in the revenue calculation of the same visitor's request in the subsequent game. As the number of visits by the visitor's access to private information increases, the amount of information the visitor can learn in LBSs may increase according to the superposition effect and the probability of revealing the privacy of the user become larger. Therefore, the same visitor's request, corresponding to the income received from different visits, is different, and the probability of good-faith access should also decrease until it is lower than the threshold imposed by the user. At this point, the visitor will no longer be allowed to access the private information of the user, according to the privacy protection strategy. This model assumes that both of the game players are rational, and the decision of the visitor and the user is in order, but the strategy adopted by the first decision-maker (i.e., the user) cannot be observed by the visitor, so it can be regarded as both decision-making, and then the game belongs to a static game model. In summary, the contributions of this work are listed as follows:

- We formally analyze the privacy protection scenarios using game theory and formulate the situation of the prisoner's dilemma game between a privacy protector (i.e., LBS user) and an outside observer (i.e., user's private information requester or simply a visitor) in a static game context.
- We analyze the existence of Nash equilibrium solutions for privacy protection methods and propose a game strategic selection to help users and outsiders obtain the corresponding benefits.
- We describe the procedures involved in the game model, the gameplay scenario, as well as the framework design used in the game theoretic model.
- We conduct some experiments based on game theory and the existing technical-oriented solutions, and we then validate the effectiveness of the former through comparison analysis.

The rest of this paper is structured as follows: First, we present an overview of a common LBS system deployment scenario and assumptions in Section 2. In addition, we discuss the adversarial consideration and game-play analysis in the traditional protection model. In Section 3, we discuss the privacy game analysis using the game theory model, so as to obtain the prisoner's dilemma, faced by both the LBS user and visitor in the traditional protection problems. Moreover, we discuss the detailed game process implementation and the framework design using game theory. Section 4 presents the evaluation analysis and comparative study through experiments to assess the effectiveness and superiority of the proposed game model. Finally, we present related work in Section 5 and summarize this work in Section 6.

2. System Model and Assumptions for LBSs

In this section, we first explain a common LBS architecture based on the probabilistic system framework proposed in [7,20] and its diverse entities, as well as our assumptions. A typical LBS application operates in a centralized fashion, i.e., the location information collected by the mobile devices of users are reported (using wireless communication infrastructures) at a central location server for processing, as illustrated in Figure 1. As shown, the basic architecture of this LBS application consists of the following four major components: (a) LBS users with smartphone devices; (b) positioning services, based on localization infrastructure; (c) communication networks (channels); and (d) third-party service providers.

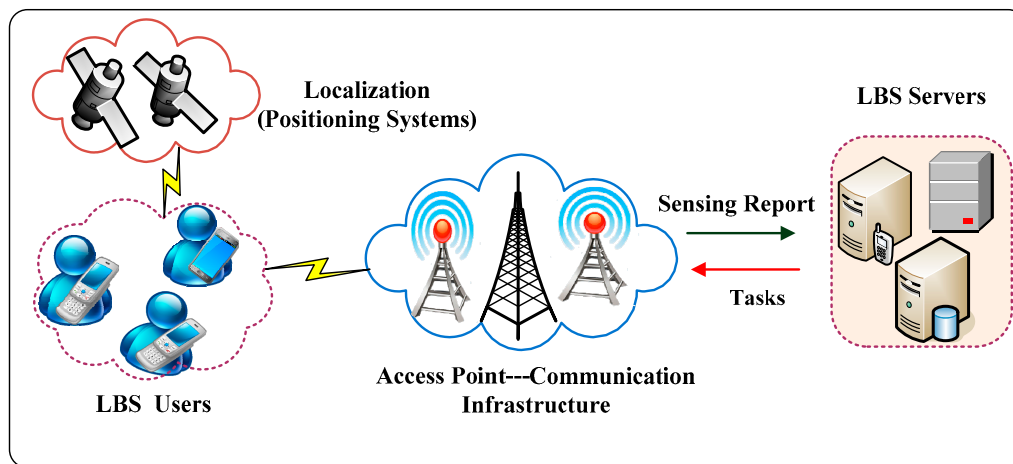


Figure 1. The common location-based service (LBS) system deployment scenario: LBS servers, localization, communication networks, and mobile users.

During the normal operation of the LBS application, each user needs to report their location-related information to the third-party LBS provider in order to receive the service. The Smartphone devices, used by LBS users, are capable of embedding a variety of positioning systems (e.g., GPS) to identify current geographic locations and other information. Moreover, they can produce a wireless connection through communication channels (e.g., a cellular network), transmit an LBS query and then return the query result from the service providers.

As for the LBS server, the location data are analyzed, associated with nearby points of interest in their databases and made available in various forms, such as a graphical representative set of positions on a map or maps, showing the location trace results at the individual and/or community level. Simultaneously, users' LBS query results may be displayed locally on their mobile devices or accessed by third-party adversarial entities through mobile and wireless networks, depending on the location information and application needs. Since the location server (such as the LBS provider) is not trusted, users' sensitive information, attached to their location trace, may be leaked or misused. In order to protect their privacy, users' usually do not directly interact with an LBS server but prioritize the query by obfuscating the privacy protection mechanism. The privacy of LBS users in a mobile network can be preserved using different protection mechanisms. To simplify privacy protection, the generic LBS adversary model assumes that the third-party service provider is malicious or untrustworthy, while other parts, such as system location privacy-preserving mechanisms (LPPMs), are secure and trusted. For privacy protection purposes, each LBS user's identity part is normally represented by a pseudonymization in LBS providers, in order to increase the adversary's uncertainty of the user's actual whereabouts. These pseudonyms might change at any time, when the users' access the LBS, or they will keep it for a longer time in order to have a long-term pseudonym. The possibility of changing each pseudonym in accordance with a set of regions depends on the LBS. It is either generated in a distributed architecture or obtained from an offline central authority [10].

2.1. Privacy and Adversarial Consideration in LBS

The goal of the adversary is to construct the location access profile of the user's target and then infer their private information (secret) based on their demographic positions. The adversary can also be the LBS provider itself or untrusted third-party entities in the LBS communication network, capturing the users' location-related information. As stated before, an adversary may have some side information about the users' LBS access pattern that aims to disclose their real-time location data and then infer their secret. Therefore, while the users' access to the various LBSs contributes to real-world mobile network sensing applications, their location privacy may leak in one of three major parts (points), i.e., user's mobile devices, communication networks and location server by itself [21,22]. According to the LBS architecture, the third-party service provider is generally considered malicious or untrustworthy. After obtaining the user's movement, an untrusted LBS provider may directly invade the user's privacy and perform localization attacks or secretly sell his/her private information to other parties [23,24].

For example, consider that mobile users use their Smartphone to request a "query to visit the nearest tumor hospital" in order to obtain some services. In this case, the LBS servers receive the LBS query from the user and reply with the query result. Let U be the LBS user's personal sensitive information that the adversary aims to track continuously over space and time and then make illegal benefit from by leveraging this information. We also assume that an adversary A can observe all the users' trajectories in their visits to the nearest tumor hospital. Furthermore, the adversary may also acquire some side information about U and may have knowledge of the protection mechanism used by the user. Because users are publicly observable by the third-party LBS provider even if they travel in public places over short periods of time. At one time location, information is identifiable, and this may reveal a detailed profile of the person's preferences, lifestyle, and habits. We note that the idea behind the traditional protection model design is applicable to LBSs, where users allow his/her trajectory observer to access their private information to a certain extent and where they deny further access when the disclosure of their privacy is about to happen.

2.2. Game Analysis in the Traditional Privacy Protection Model

In the traditional game theory model, both of the game players are still the mobile user (i.e., the owner of the location data) and the third-party visitor (who may also be the adversary), who strives to access the user's private information. The privacy protection model realizes the benefits of both players from the point of view of the "good-faith access" or "malicious access" strategy (for the user's private information visitor) and the "allow access" or "deny access to their private information" strategy (for LBS users). In the following, we define the corresponding gain and losses of both privacy game players, when they adopt different strategies:

D1-the definition of the user's income (Q_{inwel}^{acp}): The user's benefit, obtained by the visitor when an observer adopts a "good-faith access" to the user's trajectory, while the user adopts the "allow access" strategy. This benefit can also be a loss of the user, when the third-party observer adopts the "good-faith access" strategy, while the user adopts the "deny access to his private information". On the other hand, it can be seen as having the purpose of providing certain services or expanding the scope of influence by the user by allowing the outsiders to access their private information.

D2-visitor's income (B_{inwel}^{acp}): The visitor's benefit when a visitor adopts a "good-faith access" strategy, while the user adopts the "allow access" strategy. This benefit can be seen as a visitor acquiring certain services (knowledge) by providing access to the user's secret in good faith or deepening the knowledge of the LPPM used by the user, so that further communication between both sides can continue.

D3-user's loss ($Q_{lossmal}^{acp}$): The privacy losses suffered by visitors when a visitor adopts a "malicious access to the user's trajectory", while the user adopts the "allow access to his private information" strategy. The loss can be seen as a privacy breach of the user's location that the adversary has tolerated

more than the threshold imposed by the user, causing economic, prestige, career or other harm to the user.

D4-visitor's income ($B_{in_{mal}}^{acp}$): The visitor's benefit when an observer adopts a "malicious access to the user's trajectory", while the user adopts the "allow access to his private information" strategy. This benefit is different from the gains that the visitors receive through good-faith access and can be seen as the visitor acquiring the extra benefits that he or she expects but that exceed the tolerance of the user's privacy breach. In general, malicious access takes on a higher privacy risk, and at the same time, the revenue is greater than the benefits that the third-party observers receive through good-faith access.

D5-income obtained by the visitor ($Q_{in_{mal}}^{den}$): The user's benefit when a visitor adopts a "malicious access to the user's trajectory", while the user adopts a "deny access to his private information" strategy. This benefit can be seen as the user successfully protecting his or her private information against a malicious attacker by providing only a probabilistic belief of the user's private information to the LBS provider. In this case, the LBS user does not want visitors to gain through malicious access.

Obviously, when both sides of the game players adopt the "good-faith access" and the "allow access" to the user's trajectory strategies, they can establish a long-lasting information sharing relationship, which helps the two sides understand each other and cooperate. For instance, when both sides adopt the "malicious access" and the "allow access" strategies, the unilateral trust on the user side provides a convenient condition for the third-party observer to maliciously access the private information that exceeds the tolerance of the threshold imposed by the user. As a result, it brings privacy losses to the service user and additional benefits to the outsider (visitor). On the other hand, when the third-party visitor adopts the "good-faith access to the user's trajectory", while the user takes the "deny access to his private information" strategy, the rejection of the LBS user makes the visitor unable to obtain any revenue, and the user also loses the service due to his own rejection strategy, or the opportunity to expand the influence is also a loss to the LBS user. Furthermore, when the third-party visitor adopts the "malicious access" strategy and the user takes the "deny access to his private information" strategy, the user successfully protects his or her private information, and the visitor does not obtain the user's secret. As a result, the user obtains a certain benefit, and the visitor did not receive any benefit. Unfortunately, in an open network, the mobile user is unable to take any punitive measures against the third-party visitor's malicious access behavior.

Based on the above analysis, the reward matrix between the LBS user and third-party visitor in the traditional game theory model can be depicted in Table 1. It indicates that the traditional model only considers the impact of the third-party visitor's access to the user's trajectory this time. As a consequence, ignoring the characteristics of the association and superposition of private information obtained by multiple visits, even if it is more the results of a second-time visit may also result in a leak of private information by the visitor that exceeds the tolerance imposed by the user. At the same time, the lack of punishment also makes the users lose the means to protect their private information, so that visitors can make malicious visits without any concern and without worrying about any adverse consequences for themselves.

Table 1. Analyzing the reward matrix in the traditional privacy protection model.

Owners (Users)	Third-Party Visitors			
	Good-Faith		Malicious	
Allow	$Q_{in_{wel}}^{acp}$	$B_{in_{wel}}^{acp}$	$-Q_{loss_{mal}}^{acp}$	$B_{in_{mal}}^{acp}$
Refuse	$-Q_{in_{wel}}^{acp}$	0	$Q_{in_{mal}}^{den}$	0

2.3. Reward Matrix for the Traditional Game Theory Model

The goal of the adversarial third-party observer is to identify the real location and pseudonym associations in the LBS query data based on other channel matching or side information and to access the complete sensitive information related to LBSs. A descriptive example is shown in Table 1 to

analyze the privacy protection problem between the user and the third-party visitor accessing the user's private information.

The consequence of the game matrix in Table 1 can be analyzed using the line drawing method. From the perspective of the third-party observer, when the user selects the "allow access to his/her trajectory", the third-party observer "selfishly or maliciously accesses the user's secret" and will bring greater benefit to him/herself, i.e., $B_{in_{mal}^{acp}} > B_{in_{wel}^{acp}}$. At the same time, when the user selects the "deny or refuse access to private information" strategy, the "malicious access" and the "good-faith access to the user's secret" strategies have the same benefits for the visitor (i.e., both are 0). From the perspective of the LBS user, when the visitor chooses the "good-faith access to the user's secret", the "allow access" strategy can bring greater benefit to the user, i.e., $Q_{in_{wel}^{acp}} > -Q_{in_{wel}^{acp}}$. On the other hand, when the visitor chooses a "malicious access" strategy, the "deny access" mechanism can bring greater benefit to the user, i.e., $Q_{loss_{mal}^{den}} > -Q_{loss_{mal}^{acp}}$. Therefore, the analysis shows that there is a pure NE strategy set in the game matrix ($Q_{loss_{mal}^{den}}, 0$). The pure NE strategy set of the user and the visitor refer to all available sets that they are able to take. In the NE game strategy, this available set contains: "reject access" or "malicious access" to the user's private information. Let the corresponding game strategy for a player P_i be described as $S_i \in \{\text{reject, malicious}\}$.

Obviously, the NE contradicts the basic principle of information exchange and sharing, advocated in the mobile network. Even the location information related to the user's privacy is not allowed any disclosure but cannot exceed the tolerance of the threshold level imposed by the user's personal privacy strategy. Therefore, the majority of mobile network users are not always able to choose this balancing strategy. The optimal choice is contrary to the original intention of both players in the game. This is the prisoner's dilemma between the third-party observer and the LBS user in the traditional game theory model. In the next section, we will use the game theory model to solve the problem of the prisoner's dilemma game between the third-party observer and the LBS user.

3. Privacy Game Analysis using the Game Theory Model

In this section, we adopt the privacy protection scenario based on the game theoretic model to solve the prisoner's dilemma in the traditional privacy protection model [7,25]. We formulate this game as a non-constant repeated game model to specify the strategic interactions between an outside visitor and privacy protector and provide this game as the relevant theory of Nash equilibrium (NE) solutions. The properties and existence of the NE, with respect to the repeated game contexts, are analyzed in detail. By making use of location information concerning historical access and considering the current access scenario, this game model records the successively visited locations through a feedback mechanism. When the outside observer visits again, the proposed model could realize the benefits based on the past access records (observation history traces) and thus derive the probability that the access is an honest one. The benefit corresponding to the optimal strategy is based on these rewards, and the NE solution is obtained. A choice of strategy by each player is an NE point that is used to obtain the probability of the good-faith access for the visitors. At the same time, the users will set a threshold through the protection strategy based on the levels of tolerance of private information leakage, which is compared with the probability of the visitor making a good-faith visit. The LBS response to location privacy games can be obtained only when the probability of a good-faith visit is higher than the quality threshold set value imposed by the user. As a consequence, the users will adopt the "allow access" strategy, otherwise, they will take the "deny access to their private information" strategy. The privacy protection threshold value is a key parameter that determines whether or not the visitor's access request is allowed. It can be set by the user, according to his or her privacy requirements or sensitivity. The range value is generally between zero and one inclusive. This threshold value reflects the degree of the user's tolerance of the privacy breach. Table 2 shows the relationship between the tolerance level and the corresponding threshold values.

Table 2. Relationship between the degree of private information leakage and threshold values.

Tolerance	Threshold
Very High	[0, 0.2]
High	(0.2, 0.4]
Medium	(0.4, 0.6]
Low	(0.6, 0.8]
Very Low	(0.8, 1]

When this value is not set, the threshold can be set by default to the average value of 0.5. The LBS response can dynamically set this threshold according to the dynamic state of the network environment and the tolerance of private information leakage. In the process of the visitor's access to the user's trajectory, when the likelihood or probability of the good-faith visit is higher than the quality threshold value, the visitor's request will be allowed. Otherwise, the probability of good-faith access is lower than the threshold, and consequently, the request will be rejected by the user's privacy protection mechanism.

3.1. Game Theory-Based General Privacy Protection Model

Figure 2 illustrates the general process of accessing the user's private information, in which the proposed game model is used to analyze the protection strategy, based on the observation history traces and the current access scenarios of the whole LBS accessing system. Apparently, when the visitor makes an access query, the accessed location information is analyzed as to whether to allow the query, and an appropriate protection strategy will be applied by users.

Considering the current and historical access scenarios, the following procedures are available to apply the game theory-based model. (1) The visitor gathers information from users' trajectories and initiates an access request to visit their private information. (2) The system knows the private information that the visitor requests to access and obtains the private information that the visitor has visited from the historical database. (3) The system combines the various pieces of information about users in step 2 to obtain a set of private information that the visitor can access through the visit, i.e., calculate the superposition effect on the access request. (4) Based on the previous visits, the income corresponding to the different strategies adopted by the visitor and the user is calculated. (5) Based on the different strategies and calculated responses, both the visitor and the user adopt different game strategies that are used to determine the probability of the visitor's good-faith access. (6) The Nash Equilibrium solution is obtained from the privacy game between the two players. From the NE, the expected value of both players and the probability of selecting each game strategy can be obtained. (7) The proposed model determines whether the access to private information strategy is an honest one (i.e., the probability of the visitor's "good-faith access" strategy can be obtained). (8) The system compares the probability that the visitor adopts the "good-faith access to the user's trajectory" with the access threshold set by the user. If the former is not less than the latter, the "allow access" strategy is adopted. The combination of the private information, obtained by the current access and from the historical observation database, does not exceed the tolerance level of the privacy breach, otherwise, the "refuse access" strategy is adopted. In this case, the visitor could obtain the user's private information only in the history access records. (9) Finally, the results obtained by multiple visits are recorded in the historical database and applied in subsequent access decisions. When the visitor makes an access request again, the observation history data, recorded in this step, will affect the revenue of both players through steps 2 to 4, thereby affecting the LBS user's decision to adopt the "allow access" strategy or "reject (deny) access to private information strategy".

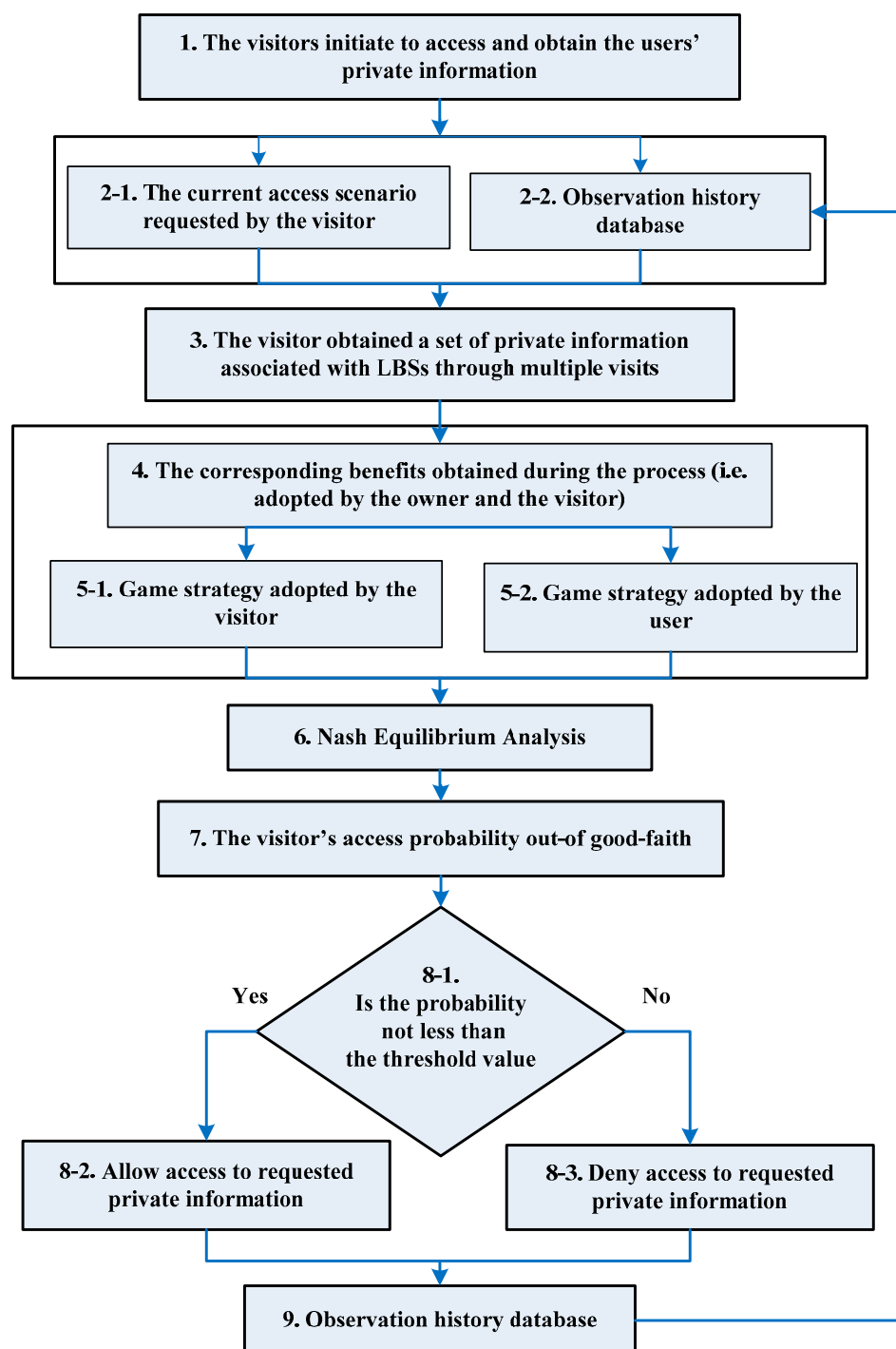


Figure 2. Proposed game-theory privacy protection model.

The flow chart in Figure 2 shows that the observation history data, recorded by the access feedback mechanism, and the setting of the threshold value may prove undesirable if the user's secret is observed by the visitor through the observation and the history traces that have already been obtained. The disclosure of the leaked private information means that the visitor adopts the "malicious access to the user's private information" and the user will not only disallow the visitor to conduct the observation beyond the private information leakage tolerance but also access the privacy letter according to the LBS provider. The history of interest is a feedback mechanism that imposes penalties or punishments on third-party observers. Therefore, while the two players of the game model issue "malicious access" and "deny access" as their respective strategies, the users required revenue by successfully protecting

their private information, and the visitor also lost due to a punishment imposed by the system. In the next section, we describe the game process between the visitor and the user in detail.

3.2. The Gameplay Process between the Privacy Protector and the Visitor

In this section, we define the details of the game process between the third-party visitor and the user, with their corresponding benefits. Before the discussion, we first prove the existence of the NE in a finite strategic game. In the game-based privacy protection model, the strategy sets of both players (i.e., the LBS user and visitor) of the game are considered as finite strategy sets, so this is a finite strategic game. According to the NE existence theorem, the game with finite sets of the user and visitor has at least one NE in each finite strategic game [26]. It can be concluded, from this, that there is at least one NE in the game of the privacy protection model. In this finite game model, we use “ β ” to represent the discounted-payoff value of the user that obtains the future earnings. Similarly, we use “ δ ” to represent the discounted-payoff value of the visitor that obtains the future earnings. Next, we need to redefine the benefits of both sides under different game strategies.

D6-user’s income (Q'_{inwel}^{acp}): The benefit of the user when a visitor adopts a “good-faith access”, while the user adopts the “allow access to his/her private information”. This benefit is also the loss of the user, when the visitor chooses the “good-faith access” strategy, while the user adopts the “refuse to access his private information” strategy. Assuming that each time the visitor requests access to the user’s trajectory, the benefit of the user is q_{inwel}^{acp} , when the visitor requests the user’s private information for the n^{th} time:

$$Q'_{inwel}^{acp} = q_{inwel}^{acp} + q_{inwel}^{acp} \times \beta + q_{inwel}^{acp} \times \beta^2 + \dots + q_{inwel}^{acp} \times \beta^n = q_{inwel}^{acp} \times \frac{1 - \beta^n}{1 - \beta} \quad (1)$$

D7-visitor’s income (B'_{inwel}^{acp}): The visitor’s revenue when a third-party observer adopts a “good-faith access” strategy, while the user adopts the “allow access” strategy in his trajectory. Assuming that each time the visitor requests access to the private information of the user, the response of the visitor is b_{inwel}^{acp} , when the visitor requests access to the private information for the n^{th} time:

$$\begin{aligned} B'_{inwel}^{acp} &= b_{inwel}^{acp} + b_{inwel}^{acp} \times \delta + b_{inwel}^{acp} \times \delta^2 + \dots + b_{inwel}^{acp} \times \delta^n \\ &= b_{inwel}^{acp} \times \frac{1 - \delta^n}{1 - \delta} \end{aligned} \quad (2)$$

D8-user’s loss ($Q'_{lossmal}^{acp}$): The visitor’s benefit when an observer adopts a “malicious access” strategy, while the user adopts the “allow access” strategy. Assume that each time the visitor requests access to the users, the visitor’s income is $q_{lossmal}^{acp}$, and then when the visitor requests access to the private information for the n^{th} time.

$$Q'_{lossmal}^{acp} = q_{lossmal}^{acp} + q_{lossmal}^{acp} \times \beta + q_{lossmal}^{acp} \times \beta^2 + \dots + q_{lossmal}^{acp} \times \beta^n = q_{lossmal}^{acp} \times \frac{1 - \beta^n}{1 - \beta} \quad (3)$$

D9-visitor’s income (B'_{inmal}^{acp}): The visitor’s revenue when an observer adopts a “malicious access” strategy, while the user adopts the “allow access” strategy. Assuming that each time the visitor requests access to the user’s trajectory, the benefit of the visitor is b_{inmal}^{acp} , when the visitor requests access to the user’s secret for the n^{th} time.

$$B'_{inmal}^{acp} = b_{inmal}^{acp} + b_{inmal}^{acp} \times \delta + b_{inmal}^{acp} \times \delta^2 + \dots + b_{inmal}^{acp} \times \delta^n = b_{inmal}^{acp} \times \frac{1 - \delta^n}{1 - \delta} \quad (4)$$

D10-visitor’s income (Q'_{inmal}^{den}): The visitor’s revenue when an observer adopts a “malicious access” strategy, while the user takes a “deny access” strategy. Assuming that each time the visitor

requests access to users, the visitor's revenue is $q_{in_mal}^{den}$, when the visitor requests access to the user's secret for the n^{th} time.

$$Q'_{in_mal}^{den} = q_{in_mal}^{den} + q_{in_mal}^{den} \times \beta + q_{in_mal}^{den} \times \beta^2 + \dots + q_{in_mal}^{den} \times \beta^n = q_{in_mal}^{den} \times \frac{1 - \beta^n}{1 - \beta} \quad (5)$$

D11-visitor's loss ($B'_{loss_mal}^{den}$): The visitor's loss when an outsider adopts "malicious access" and "deny access" strategies at the same time. Assuming that each time the visitor requests access to the user, the visitor's response is $b_{loss_mal}^{den}$, when the visitor requests access to the user for the n^{th} time.

$$B'_{loss_mal}^{den} = b_{loss_mal}^{den} + b_{loss_mal}^{den} \times \delta + b_{loss_mal}^{den} \times \delta^2 + \dots + b_{loss_mal}^{den} \times \delta^n = b_{loss_mal}^{den} \times \frac{1 - \delta^n}{1 - \delta} \quad (6)$$

Based on the expected gain and loss analysis of the user and visitor, shown above, the game matrix for both players is shown in Table 3.

Table 3. Analyzing the reward matrix in the game-theoretic privacy protection model.

Owners (Users)	Third-Party Visitors	
	Good-Faith	Malicious
Allow	$Q'_{in_wel}^{acp}$ $B'_{in_wel}^{acp}$	$-Q'_{loss_mal}^{acp}$ $B'_{in_mal}^{acp}$
Refuse	$-Q'_{in_wel}^{acp}$ 0	$Q'_{in_mal}^{den}$ $-B'_{loss_mal}^{den}$

The reward matrix in Table 3 can be analyzed using the line drawing method. From the perspective of the third-party observer, when the user selects the "allow access" strategy, the "malicious access" strategy is adopted by the visitor. This brings greater benefit to the visitor, i.e., $B'_{in_mal}^{acp} > B'_{in_wel}^{acp}$. Similarly, when the user selects the "deny access" strategy, the benefits of adopting the "malicious access" strategy for the visitor is less than the benefit of adopting the "good-faith access" strategy, i.e., $-B'_{loss_mal}^{den} < 0$. From the perspective of the LBS user, when the visitor chooses the "good-faith access" strategy, the "allow access" strategy can bring extra benefits to the user, i.e., $Q'_{in_wel}^{acp} > -Q'_{in_wel}^{acp}$. Similarly, when a third-party LBS observer chooses the "malicious access" strategy, the "deny access" strategy can bring more benefits to the user, i.e., $Q'_{in_mal}^{den} > -Q'_{loss_mal}^{acp}$. From the overall analysis, we find that there is no pure strategy NE point in the reward matrix. Therefore, we need to calculate its mixed strategy NE (randomization) solution. The randomized or mixed strategies allow each player to choose a probability of playing each allowable strategy.

We use Pr_B and Pr_Q to represent the reward (income) matrix of the visitor and the user in Table 4. Assuming that the probability of the user selecting the "allow access" strategy is x , and the "deny access" strategy is $1 - x$, the probability of the mixed strategy for the user is $Pr_Q = (x, 1 - x)$. Similarly, assuming that the probability of the third-party LBS observer selecting a "good-faith access" strategy is y and a "malicious access" strategy is $1 - y$, the probability of a visitor's hybrid strategy is $Pr_B = (y, 1 - y)$. Now, we can assume that there are N -players in the n -user game. The game's income function E_Q of the user can be determined by Equation (7), shown below:

$$\begin{aligned}
 E_Q &= Pr_q \times Pr_Q \times Pr_b^T = [x \quad 1 - x] \begin{bmatrix} Q'_{in_wel}^{acp} & -Q'_{loss_mal}^{acp} \\ -Q'_{in_wel}^{acp} & Q'_{in_mal}^{den} \end{bmatrix} \begin{bmatrix} y \\ 1 - y \end{bmatrix} \\
 &= (2x - 1) \times y \times Q'_{in_wel}^{acp} + x \times \left(-Q'_{loss_mal}^{acp} \right) \times (1 - y) + (1 - x) \times (1 - y) \\
 &\quad \times Q'_{in_mal}^{den}
 \end{aligned} \quad (7)$$

Table 4. Number of visits and private information leakage probability.

No. Visits.	Private Information Leakage Probability	
	Traditional Model	Game Theoretic Model
1	0.05	0.01
2	0.05	0.03
3	0.05	0.04
4	0.08	0.06
5	0.14	0.08

Here, E_Q reduces x , and we can get Equation (8) as follows:

$$\frac{\partial E_Q}{\partial x} = 2 \times y \times Q'_{inwel}{}^{acp} - (Q'_{lossmal}{}^{acp} + Q'_{inmal}{}^{den}) \times (1 - y) \quad (8)$$

Assuming that Equation (8) is equal to 0, and the value of y can be obtained, Equation (9) can be expressed as follows:

$$y = \frac{\frac{Q'_{lossmal}{}^{acp} + Q'_{inmal}{}^{den}}{2 \times Q'_{inwel}{}^{acp} + Q'_{lossmal}{}^{acp} + Q'_{inmal}{}^{den}} + q_{lossmal}{}^{acp} \times \frac{1 - \beta^n}{1 - \beta} + q_{inmal}{}^{den} \times \frac{1 - \beta^n}{1 - \beta}}{(2 \times q_{inwel}{}^{acp} \times \frac{1 - \beta^n}{1 - \beta} + q_{lossmal}{}^{acp} \times \frac{1 - \beta^n}{1 - \beta} + q_{inmal}{}^{den} \times \frac{1 - \beta^n}{1 - \beta})} = \frac{q_{lossmal}{}^{acp} + q_{lossmal}{}^{den}}{q_{inwel}{}^{acp} + q_{lossmal}{}^{acp} + q_{inmal}{}^{den}} \quad (9)$$

Similarly, the visitor's response E_B can be calculated by Equation (10) as follows:

$$\begin{aligned} E_B &= Pr_q \times Pr_B \times Pr_b^T = [x \quad 1 - x] \begin{bmatrix} B'_{inwel}{}^{acp} & B'_{inmal}{}^{acp} \\ 0 & -B'_{lossmal}{}^{den} \end{bmatrix} \begin{bmatrix} y \\ 1 - y \end{bmatrix} \\ &= x \times B'_{inwel}{}^{acp} \times y + x \times B'_{inmal}{}^{acp} \times (1 - y) + (1 - x) \times (-B'_{lossmal}{}^{den}) \times (1 - y) \end{aligned} \quad (10)$$

E_B derives y , and we can get Equation (11) as follows:

$$\frac{\partial E_B}{\partial y} = x \times (B'_{inwel}{}^{acp} - B'_{inmal}{}^{acp} - B'_{lossmal}{}^{den}) + B'_{lossmal}{}^{den} \quad (11)$$

$$\begin{aligned} x &= \frac{B'_{lossmal}{}^{den}}{B'_{inwel}{}^{acp} + B'_{lossmal}{}^{den} - B'_{inmal}{}^{acp}} \\ &= \frac{b_{lossmal}{}^{den} \times \frac{1 - \delta^n}{1 - \delta}}{(b_{inmal}{}^{acp} \times \frac{1 - \delta^n}{1 - \delta} + b_{lossmal}{}^{den} \times \frac{1 - \delta^n}{1 - \delta} - b_{inwel}{}^{acp} \times \frac{1 - \delta^n}{1 - \delta})} \\ &= \frac{b_{lossmal}{}^{den}}{b_{inmal}{}^{acp} + b_{lossmal}{}^{den} - b_{inwel}{}^{acp}} \end{aligned} \quad (12)$$

Therefore, the expected mixed strategy result of the NE solution is shown in Equation (13):

$$\begin{bmatrix} x & 1 - x \\ y & 1 - y \end{bmatrix} = \begin{bmatrix} \frac{b_{lossmal}{}^{den}}{b_{inmal}{}^{acp} + b_{lossmal}{}^{den} - b_{inwel}{}^{acp}} & 1 - \frac{b_{lossmal}{}^{den}}{b_{inmal}{}^{acp} + b_{lossmal}{}^{den} - b_{inwel}{}^{acp}} \\ \frac{q_{lossmal}{}^{acp} + q_{inmal}{}^{den}}{2 \times q_{inwel}{}^{acp} + q_{lossmal}{}^{acp} + q_{inmal}{}^{den}} & 1 - \frac{q_{lossmal}{}^{acp} + q_{inmal}{}^{den}}{2 \times q_{inwel}{}^{acp} + q_{lossmal}{}^{acp} + q_{inmal}{}^{den}} \end{bmatrix} \quad (13)$$

From the mixed strategy NE solution, shown above, we can understand that the protection model can obtain the probability that, when the LBS user selects the “allow access” strategy, the visitor will choose the “good-faith access” strategy in relation to the user's private information. Since the user sets an access threshold in the LPPM, according to the degree of tolerance of the user to the private information leakage, the probability that the visitor chooses the “willingly access the private information” strategy is compared with the access threshold. If the probability is not less than the threshold, the user allows the access request, otherwise, he/she rejects the visitor's access request.

3.3. Design Framework for the Game-Theoretic Protection Model

In this section, we illustrate the general framework design of game theory-based privacy protection model and point out its main components. After analyzing the game process and corresponding benefits to each player, Figure 3 illustrates a concrete design framework for the privacy protection model. In general, the designed framework consists of creating the LBS applications according to the requirements, such as executing several access tasks and actions (e.g., collecting, and controlling) on the mobile device of an LBS user, computing and reporting decisions, and storing the observed data. Inspired by the general trust model for the decision-making framework, proposed in [25], we further divide the architectural design of the game model into three phases: user's LBS access task execution, private information decision-making system, and observation history access database, as shown in Figure 3. The task execution phase mainly includes collecting the basic access information to third-party observers on the mobile device of an individual user and executing the access control decision of LBS users. As shown, the task execution part mainly includes an information acquisition module and a decision execution module. The private information acquisition module is responsible for collecting the user's location and private information requested by the visitor and providing the information to the decision-making part. The decision execution module is responsible for receiving the final decision result of the feedback for making and executing decisions.

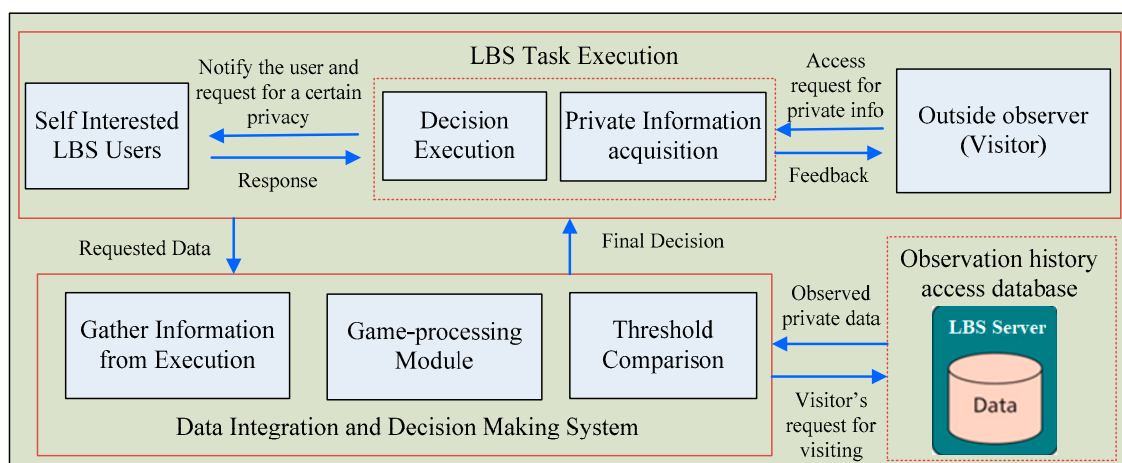


Figure 3. A Framework Design of the game-theory based privacy protection model.

The decision-making phase mainly includes receiving the basic access information, collected in the execution phase, calculating the access control decision result through a series of related algorithms and submitting the result to the execution section, and recording the private information observed by the visitor in the observation history access database. The game theory decision-making part includes three sub-modules: information gathering and collection module, game-processing module, and threshold comparison module. The private information gathering and collection module is responsible for receiving observed information, provided by the execution part, and the observation history trace, accessed by the visitor in the historical access database and combining them to calculate the visitor through the access visits. The game-process module is responsible for calculating the mixed strategy NE in the game between the third-party visitor and the user and then calculating the probability of the visitor choosing the “good-faith visit” strategy through the mixed NE strategy. The threshold comparison module is responsible for comparing the probability that the visitor, obtained by the game module, adopts the “good-faith access” strategy with the threshold set by the user in advance, and if the former is not less than the latter, the “allow access to private information” strategy is chosen. Otherwise, the “reject access” strategy is implemented, and the decision is provided to the execution module. Finally, the observation history access database is mainly responsible for storing the user's

private data, observed by the visitor, for use in decision-making and the calculation of the access control decision.

4. Experimental Analysis and Discussion

This section presents the experimental analysis to assess the performance of the proposed game theory-based privacy protection model and traditional access control solutions by leveraging the realistic mobility datasets. In Section 4.1, we present some theoretical discussions on existing traditional privacy protection mechanisms in comparison with the game theory-based protection model. Our evaluation results are demonstrated against a random approach, where the owner of the private information randomly decides whether to allow the request of the visitor to access their private information to some extent. The evaluation results and discussions of this analysis are presented in Section 4.2.

4.1. The Scenario Settings of the Evaluation System

In this paper, we take a different approach, studying privacy protection from the perspective of behavioral interest and the game-theoretic model, and we establish a privacy protection mechanism in LBS applications. The visited user's trajectory could be used to identify the users' exact positions and their private information in the other publicly available datasets. The existing research works demonstrate that privacy protection mechanisms, based on technical-oriented mechanisms (collectively referred to herein as traditional models) [13,16–18,27–29], merge analogous privacy protection strategies with existing information security-oriented access control models. The existing access control strategy reflects the necessity of privacy protection and information security techniques and then use the traditional user access control strategies, according to the identity, role, attribute or contexts, to authorize access requests, established access control policies, and the making of decisions that allow or refuse access to private information. The particular process of empowering the visitor's access inquiry still comes after the outside visitor requests to access the private information, and the accessed object (the owner) controls the request based on the privacy protection strategies. Therefore, these traditional privacy protection mechanisms based on the access control model naturally inherit the feature of independently authorizing each access inquiry and usually ignore the important requirements of privacy protection based on the features of preventing visitors from accessing users' information many times. The visited user's trajectory is superimposed to ultimately obtain the private information, and the user dynamically develops a privacy protection strategy in real time to ensure that the private information acquired by the visitor does not exceed the level of personal private information leakage tolerated by the visitors. The difference between these protection models and the game-theoretic approach is that the traditional solution usually ignores other important characteristics of privacy protection and only decides whether the visitor's current access inquiry is a malicious or honest one. From the game-theory perspective, the strategies adopted by the privacy game players and the corresponding benefits are analyzed to establish a privacy game model, and finally, the protection model adopts the visitor's good-faith access in agreement with the threshold value imposed by the user.

4.2. Data Set and Evaluation Results

In this experiment, we use the real mobility dataset from the Geolife project [30,31] to simulate the proposed game theory-based model and traditional access control solutions. This dataset contains a large number of moving trajectories of mobile users (i.e., around 17,621 identified trajectories). They were collected from 182 users over three years. In this analysis, we randomly choose 20 self-interested LBS users and 100 outsiders to visit the users' trajectories. The users randomly tag multiple pieces of private information as sensitive personal data, i.e., not expected to be leaked. When the third-part visitor successfully accesses private information that exceeds the degree of tolerance of the user, it will cause all aspects of private information about the users to be leaked. In the first experimental analysis, we observe that the visitors use the traditional and game theory-based privacy protection

models to examine the user's private information and the effectiveness of them for privacy protection. The characteristics of both protection solutions and the comparison analysis are shown in Figures 4–6, respectively. Hence, in order to obtain equitable evaluation results, we ask the outside visitor to randomly observe the user for 100 successive visits in a row, and we randomly extract 30 successive visits to analyze the privacy protection effects of a certain collection of the user's private information. Moreover, we repeat this analysis around 50 times and then extract the average of these 50 evaluation results as the final experimental outputs. Table 4 shows the relationship between the user's private information leakage probability and the number of visits in the experiment. We estimate the validity of privacy protection using Equation (14), where ρ is the probability of privacy breach, and ϵ is the validity of privacy protection.

$$\epsilon = \left(\frac{1}{2}\right)^{\rho-1} - 1 \quad (14)$$

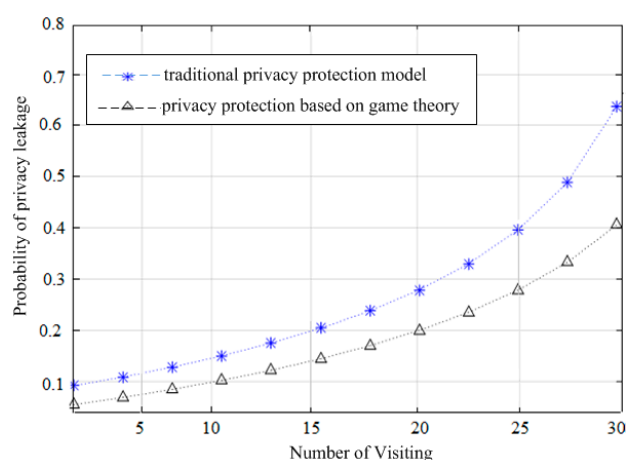


Figure 4. The probability of private information leakage between the traditional and game theory-based privacy protection models.

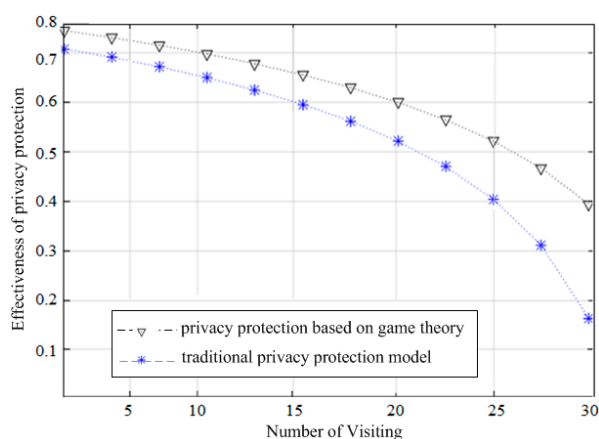


Figure 5. Comparison of the privacy protection between the traditional and game-based protection models.

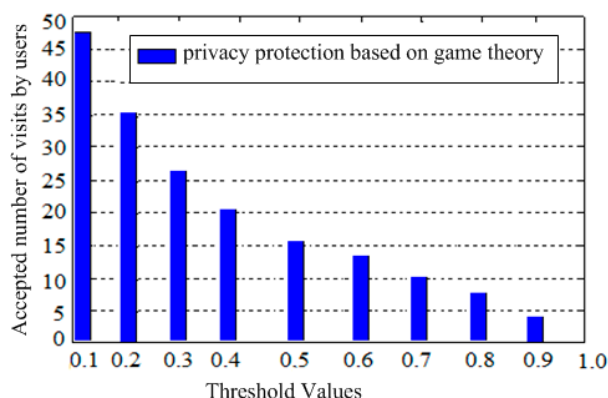


Figure 6. Relationship between the threshold values and tolerance of game theory-based privacy protection model.

The results are shown in Figure 4. As can be seen, as the number of location access increases, the traditional and game theory-based privacy protection models increase the leakage of private information probability.

This is due to the increasing number of successive visits and the additive effect of the visited user's trajectory contents, i.e., as the number of visits increases, the probability of the user's private information leakage will increase. The level of privacy breach is tolerated, but the personal privacy revealed by combining them may also be greater than the tolerance of the user. However, in comparison with the game theory-based protection model, the probability of private information leakage in the game theory model is always lower than in the traditional privacy protection model. As shown in Figure 4, the probability of leaked private information in the traditional protection mechanism is always greater than in the proposed game-based protection model. In addition, in order to observe the relationship between the thresholds set by the user and the number of visits in the game-based privacy protection model, we still assume that there are 100 visitors and 20 users and then set the visitors for 100 consecutive random accesses. We randomly extract 70 consecutive visits to observe the number of visits by which the visitor exceeded the user's tolerance for privacy breaches of different thresholds. The threshold here refers to a value set by the user according to his tolerance of private information leakage. Different users can set different thresholds according to their tolerance of the leakage of different aspects of personal information. The "allow access to private information" strategy will be taken when the probability of a "good-faith access" strategy is above this threshold. To further ensure the accuracy and objectivity of the experimental analysis, we repeat the evaluation around 50 times and take 50 average results as the final experimental output. Table 5 shows the relationship between the threshold set by the user and the number of access results. The results are shown in Figure 5, where the effectiveness of privacy protection between the traditional and game theory-based model decreases with the increase in the number of accesses. This is also the inevitable result of the superposition effect of repeated access, i.e., as the number of visitor accesses increases, the private data acquired by the visitor will be more and more. As shown in Figure 5, the effectiveness of the traditional protection model to preserve the user's private data is reduced, while the game-based model protects the private information of the user and always better than the former.

Table 5. The relationship between the threshold imposed by the user and the number of access results.

Threshold	Number of Visits
0.1	52
0.2	40
0.3	33
0.4	28
0.5	0.5
0.6	15
0.7	10
0.8	6
0.9	3
1.0	0

Furthermore, another feature of the game theory-based protection model is the flexible setting of the privacy threshold imposed by the user. The user sets the sensitivity or the privacy information protection requirement to decide whether to allow or deny the visitor to access his/her information. This privacy threshold value is used to compare with the visitor's probability to adopt the "good-faith access to the user's private information" strategy. The "allow access to the user's trajectory" strategy is adopted only when the probability of the visitor's good-faith access is not less than the access threshold imposed by the user, otherwise, the "refuse access" strategy is adopted. Figure 6 shows that in the game-based privacy protection model, as the threshold increases, the number of visits to the user's tolerance of private information leakage is reduced, i.e., the audience is less tolerant of private information leakage. Conversely, the lower the threshold, the more visitors' good-faith access will not exceed the number of visits to protect the user's privacy, i.e., the user's tolerance of private information leakage is higher.

5. Related Works

Preserving location privacy in LBSs has attracted significant research attention, supporting a wide range of applications since their emergence in recent years. Smartphone users need to share their personal information with possibly untrusted third-party visitors or service providers in various LBSs to receive some services. In these applications, we differentiate among scenarios based on the frequency at which the mobile users access a service through mobile and wireless networks. On the one hand, there are some LBS applications that require the mobile users to access them continuously (rather than sporadically), whereas, on the other hand, the majority of LBSs have users disclose their information sporadically (rather than continuously). In these cases, there are two successive accesses of a user to the LBS access pattern, with non-negligible gaps in time. Most of the existing LBS applications, such as services that allow for nearby points-of-interest, local events or near-by friends to be identified, are sporadic, as the LBSs do not need their users to expose their location all the time [32]. The authors in [33] pointed out that a sequence of location sharing services are sporadic, i.e., sparsely distributed over time, and the adversary can identify a person over space and time. In addition, several research works have studied that location privacy, even user location data under the protection mechanism, are subject to erroneous or malicious attacks [33–37]. Specifically, with the aid of other side channels, a malicious visitor attack could identify the users' present, past, and future locations, and then infer their whereabouts in order to act to damage their well-being [7,8]. In this paper, we focus on different approaches to the study of the privacy protection issues against outside visitors who have historical access data and malicious visits.

The location of the user is available in a spatial as well as temporal form. For instance, it is possible for a visitor to obtain access to a user's current location and history traces, which is called temporal access. In other scenarios, spatial access is considered critical if the user's position is located geographically. For instance, the leak of the user's identified location over time, along with their identity, would expose their behaviors in time and their interest in places by linking and inference

attacks. Hence, these spatial and temporal resolutions, associated with the position and time of the user, are important parameters for defining location privacy. The most popular approach to achieving k -anonymity location privacy in LBS is either utilizing location obfuscation or spatial-temporal cloaking techniques [38–40]. However, the spatial-temporal cloaking approach is not appropriate for the application scenario, when users use the same pseudonym locations to a certain extent. On the other hand, location obfuscation mechanisms act as a noisy information channel between the LBS provider and the user's actual location, with the intention of confusing an adversary [41]. According to [42,43], when users want to protect their location privacy in LBSs, they include false or fixed location information, rather than the actual locations of LBS users, as service query parameters. The approaches of many works, such as [44–46], fall into this category, validating the k -anonymity privacy protection effects. Both location obfuscation and spatial-temporal cloaking techniques may impair the user's private information and quality of LBS due to reporting of the obfuscated or coarse-grained version of the location information. In this paper, we let the LBSs that enable their users to continuously access their locations to obtain their private information leakage in LBS while analyzing the privacy protection effects from the perspective of game theory and incentives. We note that the principle behind our proposed framework design is applicable to LBSs, where users dynamically develop a privacy protection strategy in order to ensure that the private information, acquired by their potential visitor does not exceed the level of private information leakage tolerated by the visitors.

Game theory is an advanced study of strategic interaction between self-interested individuals (i.e., game players). Due to the high cost of privacy risk and resource consumption issues, self-interested mobile users may not be sufficiently motivated to access all the LBS applications. In the location-privacy scenario, the game theory model is an advanced tool for analyzing the user's privacy protection problems with various LBSs [7,47,48]. In this paper, we analyze the existing technical-oriented mechanisms to preserve the privacy and protect the interests of a user that utilizes LBSs against potential intruders. In contrast to existing solutions, we propose a framework, based on and inspired by the field of game theory, to better understand the intrinsic nature of privacy protection issues. A similar approach is used by [7] in the design of a distributed dummy user generation, taking into account the non-cooperative behavior of self-interested mobile users to identify the equilibrium solutions. Our solution is different from this previous work on protecting users' private information issues. In our study, we demonstrate a privacy protection model that illustrates a procedure involved in the model, the scenario of gameplay between a privacy protector and third-party visitor, as well as a framework design of a game theory model.

6. Conclusions

With the wide use of LBS applications, more and more private information regarding users' locations are collected and shared with untrusted third-party visitors, which has raised serious privacy issues due to malicious visits. In this paper, we first discussed the existing technical-oriented mechanisms to preserve the privacy of an LBS user and analyzed their characteristics and those of different technical approaches in the prevention of user privacy information. Then, we studied the prevention of a user's private information leakage in LBSs from the perspective of the behavioral interest of mobile users and game theory. From this, we proposed a privacy protection model based on game theory to better understand the intrinsic nature of the user's location privacy protection strategy. Our proposed framework shall help users to deal with privacy concerns by giving LBS users and their potential opponents a way to negotiate with one another in relation to the access of the private information of the user based on gaming aspects and incentives. From the perspective of game theory, we realized the strategy of privacy protection by disclosing the user's trajectory to a certain extent, while denying access in cases where the disclosure of privacy was about to happen. By considering the current access scenario and making use of collected private information concerning historical access traces, the game theoretic model derives the probability that the visitor's access is honest. In this context, traditional game theory aspects, such as the existence of a Nash Equilibrium solution in a

finite strategic game, were analyzed. Based on this, we further illustrated the scenario of the gameplay between the visitor and the privacy protector as well as a framework design of the game-theoretic model. Experimental analysis shows that the proposed game-theoretic protection model can protect user privacy better than the conventional privacy protection models.

Author Contributions: M.K.T. proposed the idea of the research, conceived and analyzed the mathematical model and performed the experiment analysis. X.Y. finalized the structure and instructed M.K.T. to write and to submit the paper.

Funding: This work is supported by the National Natural Science Foundation of China (NSFC) under Grant No. 61671057.

Acknowledgments: The authors wish to thank the School of Computer and Communication Engineering at University of Science and Technology Beijing. We also pleasantly acknowledge the financial assistance and support provided by NSFC.

Conflicts of Interest: We declare that there is no conflict of interest regarding the publication of this paper.

References

1. Li, H.; Zhu, H.; Du, S.; Liang, X.; Shen, X.S. Privacy leakage of location sharing in mobile social networks: Attacks and defense. *IEEE Trans. Depend. Secur. Comput.* **2018**, *15*, 646–660. [\[CrossRef\]](#)
2. Aditya, P.; Bhattacharjee, B.; Druschel, P.; Erdélyi, V.; Lentz, M. Brave new world: Privacy risks for mobile users. *ACM SIGMOBILE Mob. Comput. Commun. Rev.* **2015**, *18*, 49–54. [\[CrossRef\]](#)
3. Yi, X.; Paulet, R.; Bertino, E.; Varadharajan, V. Practical approximate k nearest neighbor queries with location and query privacy. *IEEE Trans. Knowl. Data Eng.* **2016**, *28*, 1546–1559. [\[CrossRef\]](#)
4. Bettini, C.; Bettini, D.R. Privacy protection in pervasive systems: State of the art and technical challenges. *Pervasive Mob. Comput.* **2015**, *17*, 159–174. [\[CrossRef\]](#)
5. Ghai, V.; Sharma, S.; Jain, A. Policy-Based Physical Security System for Restricting Access to Computer Resources and Data Flow Through Network Equipment. U.S. Patent 9,111,088, 18 August 2015.
6. Wang, L.; Meng, X.F. Location privacy preservation in big data era: A survey. *J. Softw.* **2014**, *25*, 693–712.
7. Liu, X.; Liu, K.; Guo, L.; Li, X.; Fang, Y. A game-theoretic approach for achieving k-anonymity in location based services. In Proceedings of the 2013 Proceedings IEEE INFOCOM, Turin, Italy, 14–19 April 2013; pp. 2985–2993.
8. Shen, H.; Bai, G.; Yang, M.; Wang, Z. Protecting trajectory privacy: A user-centric analysis. *J. Netw. Comput. Appl.* **2017**, *82*, 128–139. [\[CrossRef\]](#)
9. Hao, Y.; Cao, H.; Bhattarai, K.; Misra, S. STK-anonymity: K-anonymity of social networks containing both structural and textual information. In Proceedings of the ACM SIGMOD Workshop on Databases and Social Networks, New York, NY, USA, 22–27 June 2013; pp. 19–24.
10. Freudiger, J.; Shokri, R.; Hubaux, J.P. On the optimal placement of mix zones. In Proceedings of the International Symposium on Privacy Enhancing Technologies Symposium, Seattle, WA, USA, 5–7 August 2009; Springer: Berlin/Heidelberg, Germany, 2009; pp. 216–234.
11. Chow, R.; Golle, P. Faking contextual data for fun, profit, and privacy. In Proceedings of the 8th ACM Workshop on Privacy in the Electronic Society, Chicago, IL, USA, 9 November 2009; pp. 105–108.
12. Andrés, M.E.; Bordenabe, N.E.; Chatzikokolakis, K.; Palamidessi, C. Geo-indistinguishability: Differential privacy for location-based systems. *arXiv*, 2012; arXiv:1212.1984.
13. Tan, X.; Yu, F. Research and application of virtual user context information security strategy based on group intelligent computing. *Cogn. Syst. Res.* **2018**, *52*, 629–639. [\[CrossRef\]](#)
14. Kalnis, P.; Ghinita, G.; Mouratidis, K.; Papadias, D. Preventing location-based identity inference in anonymous spatial queries. *IEEE Trans. Knowl. Data Eng.* **2007**, *19*, 1719–1733. [\[CrossRef\]](#)
15. Tran, M.; Echizen, I.; Duong, A. Binomial-mix-based location anonymizer system with global dummy generation to preserve user location privacy in location-based services. In Proceedings of the 2010 International Conference on Availability, Reliability and Security, Krakow, Poland, 15–18 February 2010.
16. Sun, L.; Wang, H.; Soar, J.; Rong, C. Purpose based access control for privacy protection in e-healthcare services. *J. Softw.* **2012**, *7*, 2443–2449. [\[CrossRef\]](#)
17. Lu, R.; Lin, X.; Shen, X. SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *24*, 614–624. [\[CrossRef\]](#)

18. Terzi, D.S.; Terzi, R.; Sagioglu, S. A survey on security and privacy issues in big data. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015; pp. 202–207.
19. Liu, X.; Zhou, Y. A Self-Adaptive Layered Sleep-Based Method for Security Dynamic Scheduling in Cloud Storage. In Proceedings of the 2017 4th International Conference on Information Science and Control Engineering (ICISCE), Changsha, China, 21–23 July 2017; pp. 99–103.
20. Jagdale, B.N.; Bakal, J.W. Emerging trends of location privacy techniques in location aided applications. In Proceedings of the 2014 International Conference on Contemporary Computing and Informatics (IC3I), Mysore, India, 27–29 November 2014; pp. 1002–1006.
21. Shin, K.G.; Ju, X.; Chen, Z.; Hu, X. Privacy protection for users of location-based services. *IEEE Wirel. Commun.* **2012**, *19*, 30–39. [[CrossRef](#)]
22. Zhang, X.; Gui, X.; Tian, F.; Yu, S.; An, J. Privacy quantification model based on the Bayes conditional risk in Location-based services. *Tsinghua Sci. Technol.* **2014**, *19*, 452–462. [[CrossRef](#)]
23. Shokri, R.; Theodorakopoulos, G.; Danezis, G.; Hubaux, J.P.; le Boudec, J.Y. Quantifying location privacy: The case of sporadic location exposure. In Proceedings of the International Symposium on Privacy Enhancing Technologies Symposium, Waterloo, ON, Canada, 27–29 July 2011; Springer: Berlin/Heidelberg, Germany, 2011; pp. 57–76.
24. Shokri, R.; Theodorakopoulos, G.; le Boudec, J.Y.; Hubaux, J.P. Quantifying location privacy. In Proceedings of the 2011 IEEE symposium on Security and Privacy (SP), Berkeley, CA, USA, 22–25 May 2011; pp. 247–262.
25. Abdalzaher, M.S.; Seddik, K.; Elsabrouty, M.; Muta, O.M.; Furukawa, H.; Abdel-Rahman, A. Game theory meets wireless sensor networks security requirements and threats mitigation: A survey. *Sensors* **2016**, *16*, 1003. [[CrossRef](#)] [[PubMed](#)]
26. Tanaka, Y. Constructive proof of the existence of Nash equilibrium in a strategic game with sequentially locally non-constant payoff functions. *Adv. Fixed Point Theory* **2012**, *2*, 398–416.
27. Tan, Z. A lightweight conditional privacy-preserving authentication and access control scheme for pervasive computing environments. *J. Netw. Comput. Appl.* **2012**, *35*, 1839–1846. [[CrossRef](#)]
28. Omran, E.; Grandison, T.; Nelson, D.; Bokma, A. A Comparative Analysis of Chain-Based Access Control and Role-Based Access Control in the Healthcare Domain. *Int. J. Inf. Secur. Priv. (IJISP)* **2013**, *7*, 36–52. [[CrossRef](#)]
29. Pappas, V.; Krell, F.; Vo, B.; Kolesnikov, V.; Malkin, T.; Choi, S.G.; George, W.; Keromytis, A.; Bellovin, S. Blind seer: A scalable private dbms. In Proceedings of the 2014 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 18–21 May 2014; pp. 359–374.
30. Zheng, Y.; Zhang, L.; Xie, X.; Ma, W.Y. Mining interesting locations and travel sequences from GPS trajectories. In Proceedings of the 18th international conference on World Wide Web, Madrid, Spain, 20–24 April 2009; pp. 791–800.
31. Zheng, Y.; Wang, L.; Zhang, R.; Xie, X.; Ma, W.Y. GeoLife: Managing and understanding your past life over maps. In Proceedings of the 9th International Conference on Mobile Data Management (MDM'08), Beijing, China, 27–30 April 2008; pp. 211–212.
32. Shokri, R. Quantifying and protecting location privacy. *IT Inf. Technol.* **2015**, *57*, 257–263. [[CrossRef](#)]
33. Shokri, R.; Theodorakopoulos, G.; Troncoso, C.; Hubaux, J.P.; le Boudec, J.Y. Protecting location privacy: Optimal strategy against localization attacks. In Proceedings of the 2012 ACM conference on Computer and Communications Security, Raleigh, NC, USA, 16–18 October 2012; pp. 617–627.
34. Kang, J.; Yu, R.; Huang, X.; Bogucka, H.; Gjessing, S.; Zhang, Y. Location Privacy Attack and Defense in Cloud-Enabled Internet of Vehicles. *IEEE Wirel. Commun.* **2016**, *23*, 52–59. [[CrossRef](#)]
35. Polakis, I.; Argyros, G.; Petsios, T.; Sivakorn, S.; Keromytis, A.D. Where's Wally?: Precise User Discovery Attacks in Location Proximity Services. In Proceedings of the 22nd ACM Conference on Computer and Communications Security, Denver, Colorado, USA, 12–16 October 2015; pp. 817–828.
36. Feng, H.; Shin, K.G. POSTER: Positioning Attack on Proximity-Based People Discovery. In Proceedings of the 21st ACM Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; pp. 1427–1429.
37. Li, M.; Zhu, H.; Gao, Z.; Chen, S.; Ren, K.; Yu, L.; Hu, S. All Your Location are Belong to Us: Breaking Mobile Social Networks for Automated User Location Tracking. In Proceedings of the MobiHoc 2014, Philadelphia, PA, USA, 11–14 August 2014; pp. 43–52.

38. Beresford, A.R.; Rice, A.; Skehin, N.; Sohan, R. Mockdroid: Trading privacy for application functionality on smartphones. In Proceedings of the MobiHoc 2011, Paris, France, 16–19 May 2011; pp. 49–54.
39. Rodriguez-Carrion, A.; Rebollo-Monedero, D.; Forné, J.; Campo, C.; Garcia-Rubio, C.; Parra-Arnau, J.; Das, S. Entropy-based privacy against profiling of user mobility. *Entropy* **2015**, *17*, 3913–3946. [[CrossRef](#)]
40. Shokri, R. Privacy games: Optimal user-centric data obfuscation. *Proc. Priv. Enhanc. Technol.* **2015**, *2015*, 299–315. [[CrossRef](#)]
41. Chatzikokolakis, K.; Palamidessi, C.; Panangaden, P. Anonymity protocols as noisy channels. *Inf. Comput.* **2008**, *206*, 378–401. [[CrossRef](#)]
42. Lu, H.; Jensen, C.S.; Yiu, M.L. Pad: Privacy-area aware, dummy-based location privacy in mobile services. In Proceedings of the Seventh ACM International Workshop on Data Engineering for Wireless and Mobile Access (Mobide 2008), Vancouver, BC, Canada, 13 June 2008.
43. Ardagna, C.; Cremonini, M.; Damiani, E.; di Vimercati, S.d.; Samarati, P. Location privacy protection through obfuscation-based techniques. In Proceedings of the Data and Applications Security XXI, Redondo Beach, CA, USA, 8–11 July 2007.
44. Zhu, Q.; Zhao, T.; Wang, S. Privacy preservation algorithm for service-oriented information search. *Jisuanji Xuebao (Chin. J. Comput.)* **2010**, *33*, 1315–1323. [[CrossRef](#)]
45. Jia, O.; Jian, Y.; Shaopeng, L.; Yuba, L. An effective differential privacy transaction data publication strategy. *J. Comput. Res. Dev.* **2014**, *51*, 2195–2205.
46. Huo, Z.; Huang, Y.; Meng, X. History trajectory privacy-preserving through graph partition. In Proceedings of the 1st International Workshop on Mobile Location-Based Service, Beijing, China, 18 September 2011; pp. 71–78.
47. Shokri, R.; Theodorakopoulos, G.; Troncoso, C. Privacy games along location traces: A game-theoretic framework for optimizing location privacy. *ACM Trans. Priv. Secur. (TOPS)* **2017**, *19*, 11. [[CrossRef](#)]
48. Korzhyk, D.; Yin, Z.; Kiekintveld, C.; Conitzer, V.; Tambe, M. Stackelberg vs. Nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness. *J. Artif. Intell. Res.* **2011**, *41*, 297–327. [[CrossRef](#)]



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).