# A Secure Crowdsourcing-Based Indoor Navigation System

Liang Xie, Zhou Su(✉), and Qichao Xu

School of Mechatronic Engineering and Automation, Shanghai University, Shanghai 200444, People's Republic of China
zhousu@ieee.org

**Abstract.** At present, the crowdsourcing-based indoor navigation system has attracted extensive attention from both the industry and the academia. The crowdsourcing-based indoor navigation system commendably solves the deficiencies (e.g., high cost, low accuracy, etc.) of traditional navigation methods. Unfortunately, the system that relies on crowdsourced data is vulnerable to the collusion attack, which may threaten the security of the system. In this paper, a novel crowdsourcing-based secure indoor navigation system is proposed. Specifically, we first propose a novel reputation mechanism. Then, we employ the offensive and defensive game to model the interactions between the fog service platform and responders. Next, the optimization problem of the system is established to maximize the total utility of the system. Finally, the simulation results demonstrate that the proposed system can effectively encourage responders to provide positive navigation services.

**Keywords:** Crowdsourcing · Collusion · Indoor navigation · Reputation mechanism · Offensive and defensive game

## 1 Introduction

With the rapid expansion of technologies such as internet of things (IoTs) [1], the navigation system has received extensive attention from academia and industry, since it can bring unprecedented convenience to people's travel. At present, mobile smart devices are equipped with global positioning system (GPS) for precise navigation in outdoor. However, GPS signals are attenuated and distorted when they pass through the walls and various obstacles of the building, resulting in that GPS is not suitable for indoor environments. In order to realize the stability and accuracy of the navigation system within the indoor environment, the indoor navigation enabled by crowdsourcing technology has emerged. Specifically, the crowdsourcing-based indoor navigation technology presents the following advantages: 1) The crowdsourcing-based indoor navigation system does not require the deployment of a large number of sensors, which greatly reduces manpower. 2) The crowdsourcing-based indoor navigation technology is a real-time interactive technology that can provide mobile users with real-time navigation services.


S. W. Loke et al. (Eds.): MONAMI 2020, LNICST 338, pp. 125–137, 2020.
https://doi.org/10.1007/978-3-030-64002-6_9

Although the crowdsourcing-based indoor navigation system can solve the deficiencies of traditional indoor navigation [2], security is a serious problem due to the system that depends on crowdsourced data is vulnerable to the collusion attack [3,4]. Specifically, malicious responders collude with requesters who deliberately offer the positive feedback, which can contribute to the increase of their reputation. The attack of collusion behavior may cause many detrimental effects on the crowdsourcing-based indoor navigation system. For the fog platform: it disrupts the credibility of the reputation mechanism [5] and reduces the feasibility of the fog server platform. For the normal requesters: the attack of collusion behavior leaks the privacy of normal requesters and threatens the requester's personal secure. For the normal responders: the attack of collusion behavior reduces the probability of getting a task in the future.

In order to tackle the above challenges, a secure crowdsourcing-based indoor navigation system is proposed in this paper. The main distributions are summarized as follows:

- Firstly, we propose a novel crowdsourcing-based security indoor navigation system that does not require professional equipment on site to offer fundamental location services for requesters.
- Secondly, we build an attack model in conjunction with the system background and propose a novel reputation incentive mechanism based on the behaviors of responders, which ensures the security of the system.
- Thirdly, we use the offensive and defensive game to model the interactions between the fog server platform and responders. The optimization problem of the system is established to maximize the total utility of the system. The stable equilibrium solution of the game is obtained by solving the replicator dynamic equation and using the Jacobian matrix analysis method.

The rest of this paper is organized as follows: related work is reviewed in Sect. 2. In Sect. 3, we introduce the system model. In Sect. 4, we construct the offensive and defensive game model. Extensive simulations are conducted to evaluate the performance of the proposed incentive mechanism in Sect. 5. Finally, we conclude the paper in Sect. 6.

## 2 Related Work

In order to achieve the stability and accuracy of indoor positioning and navigation system, domestic and foreign scholars have put forward a large number of indoor navigation technologies in recent years. Zhuang *et al.* [6] proposed two WiFi-based crowdsourcing positioning systems, which autonomously update the database according to the dynamic changes of the indoor environment. Xiang *et al.* [7] proposed a new mobile application framework that relies on crowdsourcing technology to provide location-based services. Li *et al.* [8] proposed two incentive mechanisms to encourage people to participate in the crowdsourcing-based indoor navigation system. Chi *et al.* [9] proposed a privacy protection mechanism combining differential privacy protection and $K$ anonymity, which can

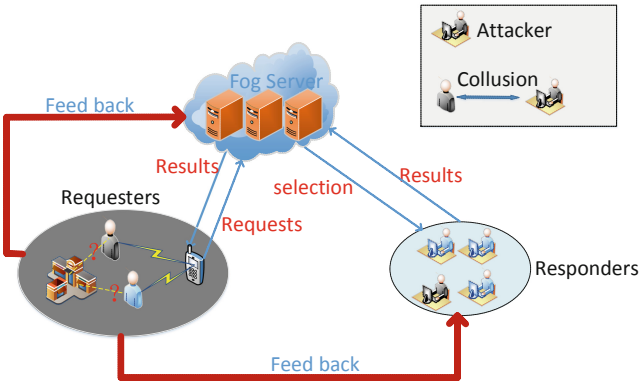


**Fig. 1.** Network model.

effectively protect the privacy of the users. Moreover, through the privacy protection mechanism, the trade-off between privacy protection and service quality is solved. Wang *et al.* [10] proposed a new method based on co-location edges, which can effectively defense the attack of attackers and improve the security of the crowdsourcing-based indoor navigation system. In summary, the above researches mainly focus on how to encourage mobile users to participate in the system. However, as the real, the security of the crowdsourcing-based indoor navigation system is the most important issue. In order to preserve the system, we propose a reputation incentive mechanism and construct the offensive and defensive game to maximize the utility of the system.

## 3 System Model

In this section, we propose the indoor navigation system consisting of four parts: network model, social relationship model, reputation mechanism, and attack model.

### 3.1 Network Model

As shown in Fig. 1, our network model is composed of the following three entities: requesters, fog server and responders.

– **Requesters** are a group of mobile users who have the requirement for navigation. We define the set of requesters as $\mathcal{U} = \{u_1, u_2, \ldots, u_I\}$. Specifically, when they broadcast tasks, the platform feeds back the navigation path provided by the responders to the requesters. After completing the task, the requesters need to pay the fee $\alpha$, where the responders obtain $\delta\%$ of the fee, the platform acquires $1 - \delta\%$. Moreover, the requesters need to feed back the reputation value $R$ to the platform and the responders. However, the requesters may be bribed by the attackers to help them attack the system.

- **Responders** are a group of mobile users who respond to a request when requesters issue a task. We define the set of responders as $V = \{\upsilon_1, \upsilon_2, \ldots, \upsilon_J\}$.
- **Fog server platform** is a completely trusted platform in the system. Meanwhile, the platform has the following functions: firstly, the platform is the connection centre between the responders and the requesters. Secondly, Fog server platform has supervision and detection abilities. If the platform choices supervision strategy, the collusion behavior of the responders can be detected with the probability of $P$.

### 3.2 Social Relationship Model

For each location request service, it is important to choose responders since the strengths and weaknesses of responders directly affect their service level. Without loss of generality, responders who have an intimate social relationship with the requester can provide better service for the requester. The social relationships between requester $i$ and responder $j$, denoted as $f(i, j)$, which are defined as

$$f(i,j) = \frac{|I_i \cap I_j|}{|I_i \cup I_j|}, \tag{1}$$

where $f(i, j) \in [0, 1]$. we define $I_i$ as a social relationship set, which is denoted by $I_i = [O_{i,1}, \ldots, O_{i,n}, \ldots, O_{i,N}]$. $O_{i,n}$ is special relationships such as friends. When these relationships exist, $O_{i,n}, = 1$ , otherwise $O_{i,n}, = 0$.

**Case 1:**

$$f(i,j) = \frac{|I_i \cap I_j|}{|I_i \cup I_j|} > HL. \tag{2}$$

The social relationship between requester $u_i$ and responder $\upsilon_j$ is intimate. $HL$ is defined as the bounds for social relationships.

**Case 2:**

$$f(i,j) = \frac{|I_i \cap I_j|}{|I_i \cup I_j|} < HL. \tag{3}$$

The social relationship between requester $u_i$ and responder $\upsilon_j$ is unfamiliar.

### 3.3 Reputation Incentive Mechanism

In the indoor navigation system, the platform provides location services to requesters by selecting responders with the highest reputation value. Moreover, based on the reputation value $R$ of the platform, requesters determine whether or not to request the platform. Therefore, some responders with low reputation value may illegally increase their reputation by colluding with the requesters.

We propose a novel reputation incentive mechanism to ensure the security of the system.

**Case 1:** When responders provide positive services. The reputation value $R$ of the platform is updated by

$$R = (1 + \epsilon) * R_0, \tag{4}$$

where $R_0$ is the initial reputation value. $\epsilon$ is the increment of reputation. In this case, we use the reputation incentive coefficient $\epsilon$ to reward responders who choose normal strategy, prompting them to persistently choose normal strategy to ensure the security of the system.

**Case 2:** When responders provide negative services, the reputation value $R$ of the platform is calculated by

$$R = (1 - \lambda) * R_0, \tag{5}$$

where $\lambda \in [0, 1]$ represents the degree of collusion. A larger $\lambda$ indicates a greater degree of collusion, resulting in a greater loss of reputation value. In this case, we use the degree of collusion of the attacker as a punishment coefficient to reduce the reputation value of the attacker and thereby reducing their utility. In this way, the attack willingness of attacker is reduced, which ensures the security of the system.

### 3.4 Attacker Model

We divide the attack model into the following categories based on several factors that affect the ability of collusion:

*1) Collusion with strangers in social relationships*

We define $\Omega$ as a collusive requester whose social relationship with the attackers is unfamiliar. When the attackers collude with $\Omega$ to attack reputation mechanism $m$ times and the number of $\Omega$ is $n$ ( $n \in [0, N]$, $m \in [0, M]$, $N \geqslant 1$, $M \geqslant 1$), attackers collaborate with $\Omega$ to issue $m$ times false mission requests. Then, $\Omega$ feeds back to the attackers with a higher reputation value, so as to influence the selection of normal requesters in the next stage.

*2) Collusion with people who are socially intimate*

We define $\Omega^\star$ as a collusive requester whose social relationship with the attackers is intimate. When the attackers collude with the $\Omega^\star$ to attack reputation mechanism $m$ times and the number of $\Omega^\star$ is $n$ ( $n \in [0, N]$, $m \in [0, M]$, $N \geqslant 1$, $M \geqslant 1$), attackers collaborate with $\Omega^\star$ to issue $m$ times false mission requests.

## 4 Offensive and Defensive Game

### 4.1 Problem Formulation

Responders are categorized into two categories: the normal responders and the attackers. The attackers collude with the requesters with a probability $x$, and illegally increase their profits with a degree of collusion $\lambda$. The collusion level $\lambda$ follows

$$\lambda = \frac{1}{1 + e^{-[f(i,j) * g(C_u, N_u)]}}, \tag{6}$$

where $\lambda \in [0, 1]$ is proportional to the capacities of attackers. $\omega$ is the accuracy of the path provided by the attackers. $g(C_u, N_u)$ is the frequency of attacks, defined as

$$g(C_u, N_u) = \sigma_1 C_u + \sigma_2 N_u, \tag{7}$$

where $N_u$ is the number of requesters who collude with the attackers. $C_u$ is the times of attacks. $\sigma_1$ is the importance of the number of colluding requesters in the attacks frequency. $\sigma_2$ is the importance of the times of attacks in the attack frequency.

The attacker also can disguise himself as a normal responder to reduce the probability of being supervised by the platform. The quality of the navigation path provided by the attackers, denoted as $\beta$, which is defined as

$$\beta = \begin{cases} \beta_{min}, & \text{if the destination is inconsistent,} \\ \frac{\int_A^B h(x,y,z)\, dl}{\int_A^B h'(x,y,z)\, dl}, & \text{if the destination is consistent.} \end{cases} \tag{8}$$

$A$ is the starting point of the path and $B$ is the end point of the path. $h(x, y, z)$ is the shortest trajectory from point $A$ to point $B$. $h'(x, y, z)$ is the trajectory from point $A$ to point $B$ provided by the attacker. The normal responder's $\beta$ is equal to 1, because the normal responder's target is to improve his utility. When the attackers choose the wrong navigation path, the value of $\beta$ is $\beta_{min}$.

The fog service platform has the functions of supervision and detection in the system. When the platform chooses the supervision strategy, it has a probability $P$ to successfully supervise the collusion behavior of the attackers. If detected, the attackers need to pay the illegal cost. Otherwise, the attackers will receive illegal income, which is the platform losses. The probability of platform successful supervision $P$ follows

$$P = (1 - \beta\lambda). \tag{9}$$

When the platform supervision fails, it is considered that the attackers choose the non-collusion strategy.

### 4.2 Utility Function

The offensive and defensive game matrix is shown in Table 1.

**Table 1.** The offensive and defensive game matrix

| | | Fog serve platform | |
|---|---|---|---|
| | | (y)supervision | (1-y)non-supervision |
| Responders | (x)collusion | $U_a(x,y), U_d(x,y)$ | $U_a(x,1-y), U_d(x,1-y)$ |
| | (1-x)non-collusion | $U_a(1-x,y), U_d(1-x,y)$ | $U_a(1-x,1-y), U_d(1-x,1-y)$ |

*(1) When the responders choose the collusion strategy and the degree of collusion is $\lambda$, as well as the platform chooses the supervision strategy:*

Different from the traditional definition of utility, we introduce the reputation incentive mechanism and divide the utility into current utility and future utility. The utility of the responders is defined as

$$U_a = U_a^m + U_a^n, \tag{10}$$

where $U_a$ is the total utility of the responders. $U_a^m$ is the current utility of the responders, and $U_a^n$ is the future utility of the responders.

The current utility of the responders is defined as

$$U_a^m(x,y) = \sum\nolimits_{k=1}^{k_d} [\delta\alpha_k - \lambda\beta_k c_1 - PW\lambda + (1-P)S\lambda], \tag{11}$$

where $k_d$ is the total number of tasks. $W$ represents the cost of attacker when the attack fails. $S$ represents the attacker's profits when the attack is successful. $c_1$ represents the unit cost of the responders who choose the collusion strategy.

The future utility of the responders follows

$$U_a^n(x,y) = \delta e^{\varphi R}, \tag{12}$$

where $R$ represents the reputation value of the platform. $\varphi > 0$ represents a positive correlation coefficient between reputation value and future utility.

Substituting Eq. (11) and Eq. (12) into the Eq. (10), the total utility of the responders can be rewritten as

$$\begin{aligned} U_a(x,y) = &\sum\nolimits_{k=1}^{k_d} [\delta\alpha_k - \lambda\beta_k c_1 - PW\lambda + (1-P)S\lambda] \\ &+ \delta e^{\varphi(1-\lambda)R_0}. \end{aligned} \tag{13}$$

We design a novel reputation incentive mechanism that links future utility, so as to encourage responders to choose the non-collusion strategy.

The utility of the platform is defined as

$$U_d = U_d^m + U_d^n, \tag{14}$$

where $U_d$ is the total utility of the platform. $U_d^m$ is the current utility of the platform, and $U_d^n$ is the future utility of the platform.

The current utility of the platform follows

$$U_d^m(x,y) = \sum\nolimits_{k=1}^{k_d} [(1-\delta)\alpha_k - d_1 + PJ\lambda - (1-P)B\lambda], \tag{15}$$

where $d_1$ is the cost of the platform when the platform chooses the supervision strategy. $J$ is the profits from platform successful supervision. $B$ is the cost of the platform when attackers collusion successfully.

The future utility is defined by the reputation value of the platform

$$U_d^n(x,y) = (1-\delta)e^{\varphi R}. \tag{16}$$

Substituting Eq. (15) and Eq. (16) into the Eq. (14), the total utility of the platform can be rewritten as

$$\begin{aligned} U_d(x,y) = &\sum\nolimits_{k=1}^{k_d}[(1-\delta)\alpha_k - d_1 + PJ\lambda - (1-P)B\lambda] \\ &+ (1-\delta)e^{\varphi(1-\lambda)R_0}. \end{aligned} \tag{17}$$

*(2) When the responders choose the collusion strategy and the degree of collusion is $\lambda$, as well as the platform chooses the non-supervision strategy:*

The current utility of the responders is defined as

$$U_a^m(x,1-y) = \sum\nolimits_{k=1}^{k_d}[\delta\alpha_k - \lambda\beta_k c_1 + S\lambda]. \tag{18}$$

The future utility of the responders is denoted as

$$U_a^n(x,1-y) = \delta e^{\varphi R}. \tag{19}$$

Substituting Eq. (18) and Eq. (19) into the Eq. (10), the total utility of the responders can be rewritten as

$$\begin{aligned} U_a(x,1-y) = &\sum\nolimits_{k=1}^{k_d}[\delta\alpha_k - \lambda\beta_k c_1 + S\lambda] \\ &+ \delta e^{\varphi(1-\lambda)R_0}. \end{aligned} \tag{20}$$

The current utility of the platform is defined as

$$U_d^m(x,1-y) = \sum\nolimits_{k=1}^{k_d}[(1-\delta)\alpha_k - d_2 - B\lambda], \tag{21}$$

where $d_2$ is the cost of the platform when the platform chooses the non-supervision strategy.

The future utility of the platform is denoted as

$$U_d^n(x,1-y) = (1-\delta)e^{\varphi R}. \tag{22}$$

Substituting Eq. (21) and Eq. (22) into the Eq. (14), the total utility of the platform can be rewritten as

$$\begin{aligned} U_d(x,1-y) = &\sum\nolimits_{k=1}^{k_d}[(1-\delta)\alpha_k - d_2 - B\lambda] \\ &+ (1-\delta)e^{\varphi(1-\lambda)R_0}. \end{aligned} \tag{23}$$

*(3) When the responders choose the non-collusion strategy and the platform chooses the supervision strategy:*

The total utility of the responders is defined as

$$U_a(1-x,y) = \sum_{k=1}^{k_d}[\delta\alpha_k - c_2] + \delta e^{\varphi(1+\epsilon)R_0}, \tag{24}$$

where $c_2$ is the cost of the responders who choose the non-collusion strategy.

The total utility of the platform is denoted as

$$\begin{aligned} U_d(1-x,y) = &\sum_{k=1}^{k_d}[(1-\delta)\alpha_k - d_1] \\ &+ (1-\delta)e^{\varphi(1+\epsilon)R_0}. \end{aligned} \tag{25}$$

*(4) When the responders choose the non-collusion strategy and the platform chooses the non-supervision strategy:*

The total utility of the responders is defined as

$$U_a(1-x,1-y) = \sum_{k=1}^{k_d}[\delta\alpha_k - c_2] + \delta e^{\varphi(1+\epsilon)R_0}. \tag{26}$$

For the platform, it does not need to pay more cost to manage the behavior of responders. The total utility of the platform is denoted as

$$\begin{aligned} U_d(1-x,1-y) = &\sum_{k=1}^{k_d}[(1-\delta)\alpha_k - d_2] \\ &+ (1-\delta)e^{\varphi(1+\epsilon)R_0}. \end{aligned} \tag{27}$$

### 4.3 Game Equilibrium Solution

In the replication dynamic equation, the growth rate of a strategy in the community is equal to the difference between the utility of the strategy and the average utility of the community [11]. Therefore, the replication dynamic equation can be described as

$$\begin{aligned} \frac{dx}{dt} &= x[U_a(x) - \bar{U_a}], \\ \frac{dy}{dt} &= y[U_d(y) - \bar{U_d}], \end{aligned} \tag{28}$$

where $\bar{U_a}$ and $\bar{U_d}$ are the average utility of the responders and platform, respectively. Based on the replication dynamic equations of the two parties, the equation $M$ can be described as

$$M = \begin{bmatrix} \frac{dx}{dt} \\ \frac{dy}{dt} \end{bmatrix}. \tag{29}$$

We can get five sets of equilibrium solutions by letting $M = 0$, which are $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$, $(x^*, y^*)$. The expression of $x^*$ is

$$x^* = \frac{d_1 - d_2}{P(J+B)\lambda}. \tag{30}$$

The expression of $y^*$ is

$$y^* = \frac{\delta(e^{\varphi(1-\lambda)R_0} - e^{\varphi(1+\epsilon)R_0}) - \lambda\beta c_1 + c_2 + S\lambda}{PK_d(S+W)\lambda}. \tag{31}$$

### 4.4 Stability Analysis of Equilibrium Solutions

For a group of dynamic characteristic described by a differential equation system, the stability of its equilibrium point is obtained by using the local stability analysis method of the Jacobian matrix.

**Case 1:** When $[(1-2P)S\lambda - \beta\lambda c_1 + \delta e^{[\varphi(1-\lambda)R_0]}] - (\delta e^{[\varphi(1+\varepsilon)R_0]} - c_2) > 0$ and $d_2 > d_1$, the equilibrium point of the system is only (1, 1), i.e., the responders select the collusion strategy, and the fog server platform selects the supervision strategy.

**Case 2:** When $[(1-2P)S\lambda - \beta\lambda c_1 + \delta e^{[\varphi(1-\lambda)R_0]}] - (\delta e^{[\varphi(1+\varepsilon)R_0]} - c_2) < 0$, and $2PJ\lambda + d_2 < d_1$, the equilibrium point of the system is only (0, 0), i.e., the responders select the non-collusion strategy, and the fog server platform selects the non-supervision strategy.

**Case 3:** When $[(1-2P)S\lambda - \beta\lambda c_1 \delta e^{[\varphi(1-\lambda)R_0]}] - (\delta e^{[\varphi(1+\varepsilon)R_0]} - c_2) > 0$ and $2PJ\lambda + d_2 < d_1$, the equilibrium point of the system is only (1, 0), i.e., the responders select the collusion strategy, and the fog server platform selects the non-supervision strategy.

**Case 4:** When $[(1-2P)S\lambda - \beta\lambda c_1 + \delta e^{[\varphi(1-\lambda)R_0]}] - (\delta e^{[\varphi(1+\varepsilon)R_0]} - c_2) < 0$, and $d_2 > d_1$, the equilibrium point of the system is only (0, 1), i.e., the responders select the non-collusion strategy, and the fog server platform selects the supervision strategy.

## 5 Performance Evaluation

### 5.1 Simulation Setup

In the simulations, the increment of reputation is selected from the interval $[0, 1]$. The total profit of per task is set to be 0.5. The responder's profit as a percentage of total profit is set to be 0.6. The initial reputation value is set as 0.5. The quality of the navigation path provided by the attackers is set as 0.2. Other parameters in the simulations are given in Table 2 to satisfy our four constraints. The performance of the proposed reputation incentive mechanism is verified by comparing with two mechanisms, namely the fixed mechanism and the linear mechanism.

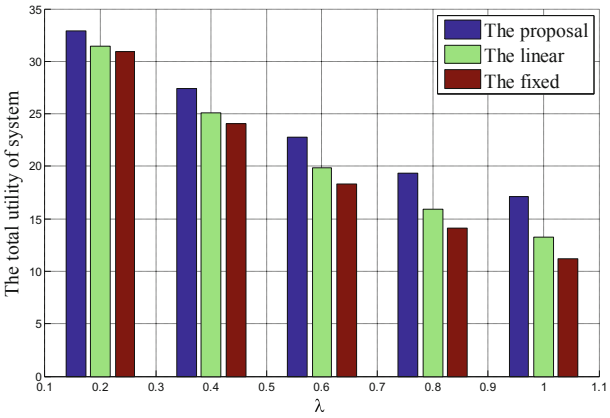


**Fig. 2.** The impacts of $\lambda$ on total utility of system.

**Table 2.** Parameters

| Case 1 | | Case 4 | |
|---|---|---|---|
| Parameter | Value | Parameter | Value |
| $S$ | 1 | $S$ | 1 |
| $W$ | 1 | $W$ | 1 |
| $J$ | 1 | $J$ | 1 |
| $B$ | 1 | $B$ | 1 |
| $c_1$ | 0.5 | $c_1$ | 0.5 |
| $c_2$ | 5 | $c_2$ | 0.5 |
| $d_1$ | 0.2 | $d_1$ | 0.2 |
| $d_2$ | 0.4 | $d_2$ | 0.4 |
| $\varphi$ | 3 | $\varphi$ | 4 |
| $K_d$ | 10 | $K_d$ | 10 |

### 5.2 Simulation Results

It is shown in Fig. 2 that the impact of $\lambda$ on total system utility. We compare the proposed mechanism with the fixed mechanism and linear mechanism to verify the effectiveness of the proposed mechanism. From Fig. 2, we can obtain that with the increase of $\lambda$, the system utilities obtained by the three mechanisms are gradually reduced, while the utilities based on the proposed mechanism are better than the utilities obtained by the other two mechanisms. The reason is that the offensive and defensive game can effectively motivate responders to pay attention to long-term utilities with reputation incentives and choose the best strategy with reputation incentive. In the fixed mechanism, the attacker chooses the strategy according to the preset probability. In the linear mechanism, the attacker chooses the strategy without considering the reputation mechanism.

Therefore, the performance based on the proposed mechanism is better than the other two mechanisms.

## 6 Conclusion

In this paper, we have proposed a crowdsourcing-based secure indoor navigation system. Firstly, we have built an attack model in conjunction with the system background, and we have proposed a novel reputation incentive mechanism. Secondly, we have constructed the offensive and defensive game to model the interactions between the fog service platform and responders. By means of game theory, the utility function of both the system and the attacker are maximized. Finally, extensive simulations have validated the effectiveness of our mechanism. For the future work, we plan to take the multi-stage collusion into account to improve the reliability of the crowdsourcing-based indoor navigation system.

**Acknowledgements.** This work is supported in part by NSFC (nos. U1808207, 91746114), and the Project of Shanghai Municipal Science and Technology Commission, 18510761000.

## References

1. Su, Z., Wang, Y., Xu, Q., Zhang, N.: LVBS: lightweight vehicular blockchain for secure data sharing in disaster rescue. IEEE Trans. Depend. Secure. https://doi.org/10.1109/TDSC.2020.2980255
2. Li, W., Su, Z., Zhang, K., Benslimane, A., Fang, D.: Defending malicious check-in using big data analysis of indoor positioning system: an access point selection approach. IEEE Trans. Netw. Sci. Eng. https://doi.org/10.1109/TNSE.2020.3014384
3. Li, W., Su, Z., Zhang, K., Xu, Q.: Abnormal crowd traffic detection with crowdsourcing-based RSS fingerprint position in heterogeneous communications networks. IEEE Trans. Netw. Sci. Eng. https://doi.org/10.1109/TNSE.2020.3014380
4. Wang, Y., Su, Z., Zhang, N., Benslimane, A.: Learning in the air: secure federated learning for UAV-assisted crowdsensing. IEEE Trans. Netw. Sci. Eng. https://doi.org/10.1109/TNSE.2020.3014385
5. Goswami, A., Gupta, R., Parashari, G.S.: Reputation-based resource allocation in P2P systems: a game theoretic perspective. IEEE Commun. Lett. **21**(6), 1273–1276 (2017)
6. Zhuang, Y., Syed, Z., Li, Y., El-Sheimy, N.: Evaluation of two WiFi positioning systems based on autonomous crowdsourcing of handheld devices for indoor navigation. IEEE Trans. Mob. Comput. **15**(8), 1982–1995 (2016)
7. Xiang, L., Tai, T., Li, B., Li, B.: Tack: learning towards contextual and ephemeral indoor localization with crowdsourcing. IEEE J. Sel. Areas Commun. **35**(4), 863–879 (2017)
8. Li, W., Zhang, C., Liu, Z., Tanaka, Y.: Incentive mechanism design for crowdsourcing-based indoor localization. IEEE Access **6**, 54042–54051 (2018)
9. Chi, Z., Wang, Y., Huang, Y., Tong, X.: the novel location privacy-preserving CKD for mobile crowdsourcing systems. IEEE Access **6**, 5678–5687 (2018)

10. Wang, G., Wang, B., Wang, T., Nika, A., Zheng, H., Zhao, B.Y.: Ghost riders: sybil attacks on crowdsourced mobile mapping services. IEEE/ACM Trans. Networking **26**(3), 1123–1136 (2018)
11. Xu, H., Wang, Z., Xiao, W.: Analyzing community core evolution in mobile social networks. In: 2013 International Conference on Social Computing, Alexandria, VA, pp. 154–161 (2013)