IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received July 31, 2018, accepted August 30, 2018, date of publication October 29, 2018, date of current version November 19, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2872740

A Trustworthy Content Caching and Bandwidth Allocation Scheme With Edge Computing for Smart Campus

QICHAO XU, ZHOU SU, YUNTAO WANG, AND MINGHUI DAI
School of Mechatronic Engineering and Automation, Shanghai University, Shanghai 200072 , China
Corresponding author: Zhou Su (zhousu@ieee.org).

This work was supported in part by NSFC under Grant 91746114 and Grant 61571286, and in part by the Shanghai Key Laboratory of Power Station Automation Technology.

ABSTRACT Edge computing enabled mobile social networks can improve mobile users' quality of experience (QoE) when they exchange and share contents with each other. However, as some edge nodes are trustless or even malicious, mobile users are attacked by these untrustful nodes. Meanwhile, due to the limited caching and bandwidth capacities of edge nodes, the competition among mobile users also brings a new challenge to allocate the resource efficiently. To tackle the above problems, this paper presents a trustworthy edge caching and bandwidth allocation scheme for mobile users. First, to guarantee the reliability of each edge node, a trust evaluation mechanism is designed to assess the security of each edge node by the direct trust and indirect trust. With the trust evaluation, each mobile user selects satisfied edge nodes as candidates to cache contents. Then, the reverse auction game is employed to find the optimal edge node for each mobile user. The Bayesian equilibrium obtained via game analysis is used to determine the optimal strategy of each edge node. Finally, the simulation results show that the proposed scheme can not only improve the QoE of mobile users, but also prevent the attacks of malicious edge nodes.

INDEX TERMS Smart campus, edge computing, trust evaluation, game theory.

I. INTRODUCTION

Smart campus applications and services have emerged with the rapid developments of wireless communication and network technologies. Especially, with mobile devices, mobile users can generate, deliver, and share contents with each other to form the mobile social networks (MSNs) [1]–[6] in smart campus. The content delivery in MSNs has become a promising alternative for mobile users to exchange multimedia data. Recent report shows that the number of mobile devices connecting to the Internet has been more than the population in the world since 2014 [7]. The rapid growth of mobile users and the ever increasing scale of MSNs provide the enormous potentials. It can be predicted that MSNs will be one of the most important network paradigms in the next generation [8]–[13], which can significantly support the realization of the smart campus.

However, recently the social content delivery in smart campus encounters a bottleneck to obtain the satisfactory performance for mobile users. Firstly, since the content servers are usually located far away from users, it brings a large latency for mobile users to retrieve the content. Secondly, the backbone is overloaded to deliver numerous duplicated contents. Edge computing technology has been advocated to tackle the above problems with a widespread attention from the industry and academia. With edge computing, the contents can be cached on the edge nodes, which are located at the edge of the network and close to mobile users. When a mobile user sends a request, if the replica of the requested content is cached on the edge node, the requested content can be delivered to the user directly with a short delay. Additionally, since contents can be directly obtained from the edge nodes instead of the remote servers, the traffic on the backbone can be also significantly mitigated [14]–[16].

Although edge computing enabled MSNs have many benefits for mobile users, it also brings following problems. On one hand, as edge nodes are deployed by rational third parties, edge nodes may maliciously conduct attacks on network. For example, malicious edge nodes inject viruses or malwares into mobile users and destroy the normal operations of the MSNs. On the other hand, due to the limited caching and bandwidth capacities of edge nodes, the caching and bandwidth resource need to be allocated efficiently for mobile users to cache desired contents. Because of the competitions among edge nodes, it is not easy for mobile user to find the optimal edge node with the satisfied resource and price to cache contents. Therefore, it is an open and important issue to design an efficient scheme for improving the security of edge caching service in smart campus.

Some existing works [17]–[19] have studied the secure caching in wireless networks. But most of them cannot be directly applied in edge computing enabled MSNs. On one hand, most of them do not focus on the edge computing technology, where the contents are distributed with the cooperations of mobile users. On the other hand, the social relationships and trust among individuals need to be analyzed for protecting the security of contents and mobile users.

Therefore, in this paper we present a trustworthy content caching scheme with edge nodes in MSNs for smart campus based on the reverse auction game. Firstly, for the realization of securely caching contents on edge nodes, a trust evaluation mechanism is introduced to assess the reliability of edge node, where the trust derivation consists of the direct trust evaluation and indirect trust evaluation. The direct trust evaluation is based on the direct historical experiences, while the indirect trust is derived from the recommendations of others. After evaluating the reliability of edge nodes, we use the reverse auction game to find the optimal decision for users to select edge nodes. With the back induction method, the Bayesian equilibrium is obtained to provide the stable caching strategies for mobile users. Finally, the simulation experiments prove that the proposed scheme can outperform other conventional schemes to provide the trustworthy content caching for mobile users.

The remainder of this paper is organized as follows. Section 2 reviews the related work. The system model is shown in Section 3. Section 4 introduces the proposed scheme. Section 5 shows the performance evaluation of the proposed scheme, and the paper is concluded in Section 6.

II. RELATED WORK

In this section, we review the related work including smart campus construction, trust evaluation management, and content caching.

A. SMART CAMPUS CONSTRUCTION

Recently, smart campus has been a hot topic in the academia and industry. Petrie *et al.* [20] designed and implemented an energy efficient control framework for heating, ventilation, and air conditioning systems of the commercial buildings for smart campus, where these systems are responsible for providing acceptable indoor air quality and thermal comfort to the occupants. Tian *et al.* [21] proposed a method to implement out-of-band data capturing for attack resistance with virtual machine introspection technique, where this scheme isolates the data captured from monitored hosts. Sivanathan *et al.* [22] presented the use of network traffic analytics to characterize Internet of Thing devices and their typical behaviour model in smart cities. Wang *et al.* [23] introduced a differential model of virus propagation for smart campus network by considering the differences among individuals and proposed a method to extend the individual evolution process to the evolution process. Qiu *et al.* [24] presented a sentiment classification method for microblogs based on multi-feature fusion by choosing smart campus as theme of Weibo texts. However, few of them consider security problems for caching contents, where a satisfactory system performance can not be obtained in real applications.

B. TRUST EVALUATION MANAGEMENT

The trust evaluation mechanism has been studied widely. Liu and Jia [25] gave the research on the trust evaluation strategy for the service provider based on the social trust inference paths between the service consumer and the service provider. Shen *et al*. [26] presented a framework to manage the trust based on a hierarchical mechanism by evaluating the trust level of a node with all group members or a trusted server. Hao *et al*. [27] inferred trust semantically among mobile users with a fuzzy inference scheme, where mobile users may not be directly connected with each other. Wang [28] proposed trustworthiness measurement scheme by the perceptions of ability, benevolence, and integrity quantitatively for cyber-physical systems. Zhu *et al.* [29] designed a scheme to enable trust-based crowdsensing services in connected vehicular cloud computing, which divides the system into control and data planes. However, the above trust management can not be directly applied in MSNs, as they don't consider the social relationships among users.

C. CONTENT CACHING

Content caching has attracted a large number of attention from the world. Zhi *et al*. [30] studied the social ties and physical distance as the factors to formulate the caching cost and proposed a social-aware caching game to motivate nodes to cache data for others. Wang *et al*. [31] proposed a Markovchain-based model to analyze edge caching among edge nodes, and data sharing scheme among the potential MSNs from the aspect of content diffusion in the fog radio access networks. Zhang *et al*. [32] focused on two layer social cyberspaces in both traffic correlation between base stations and the social relationship with user equipments. The authors proposed an information caching strategy for cyber social computing based wireless networks. Taghizadeh *et al*. [33] designed the cooperative caching policies for minimizing electronic content provisioning cost in social wireless networks. Ndikumana *et al.* [1] proposed a joint incentive mechanism and price based cache replacement policy in named data networking to improve the Internet service providers' and content providers' profits. However, most of them assume that all nodes are secure and honest, where the malicious edge nodes in MSNs should be further considered.

Therefore, this paper is to propose a novel secure edge caching scheme for multiple contents in MSNs. This work is aimed to reduce content retrieve delay for improving the QoE of mobile users and prevent the attacks of malicious edge nodes to guarantee the integrality of cached contents.

III. SYSTEM MODEL

In this section, as shown in Fig. 1, we describe the system model of the presented scheme in detail. The network model is first introduced followed by the content model. Then, the trust model is elaborated.

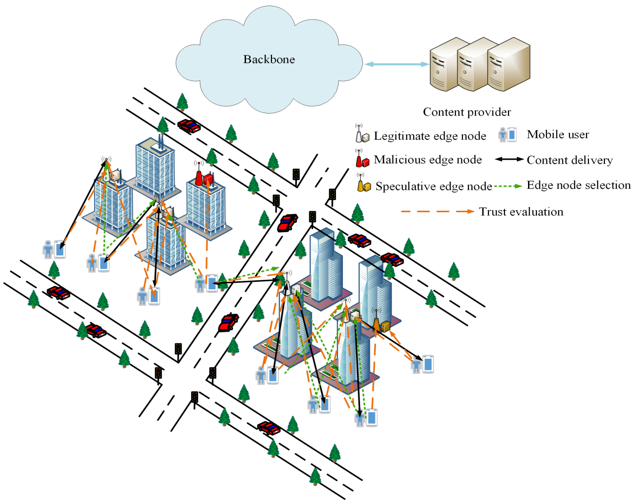


FIGURE 1. System model.

A. NETWORK MODEL

- **Content provider:** The content provider is located at the remote area. Due to the remote deployment of the content provider, it brings a large latency to fetch the content requested by a mobile user. It is assumed that there are average k route nodes in backbone network to fetch a content from the content provider. The bandwidth between two route nodes is b. The data rate of the content provider is $\tilde{b}$ and the data rate of the access point provided by the backbone is $\hat{b}$. The delay to fetch the data with unit data size from the content provider is

$$d = \frac{1}{b}(k-1) + \frac{1}{\tilde{b}} + \frac{1}{\hat{b}}. \tag{1}$$

- **Edge nodes:** Edge nodes are placed at the edge of backbone and close to mobile users. Each edge node has a certain caching capacity to store contents. Thus mobile users can obtain contents from edge nodes directly instead of the content provider. In an area such as the campus, office building, etc., the set of edge nodes is denoted by $\mathcal{I} = \{1, 2, \cdots, i, \cdots, I\}$. Mobile users are free to access edge nodes with wireless communications, while the caching services need to be charged by edge nodes. In addition, it is assumed that there are three types of edge nodes, which are legitimate edge nodes, malicious edge nodes, and speculative edge nodes, respectively. The legitimate edge nodes are those which can provide secure caching services for mobile users. The malicious edge nodes can attack and destroy the network. Speculative edge node randomly selects its mode as a legitimate or malicious one. The ratios of legitimate, malicious, and speculative edge nodes are denoted as hr, mr, and sr, respectively.
- **Mobile users:** Mobile users can generate and share contents with each other. When a mobile user discovers or generates an interesting content, he/she can upload the content to nearby edge node or deliver it directly to content provider. Meanwhile the mobile user recommends the content to his/her friends with a link via social platforms, such as Facebook, Wechat, etc. The set of mobile users in the network is denoted as $\mathcal{J} = \{1, 2, \cdots, j, \cdots, J\}$. Let $r_{j,j'}$ $(j \in \mathcal{J},\ j' \in \mathcal{J})$ denote the social relationship degree between mobile user j and j', where $0 \leq r_{j,j'} \leq 1$. If $r_{j,j'} = 1$, two mobile users j and j' have the highest social relationship. Otherwise, $r_{j,j'} = 0$. The social relationship degree matrix for all mobile users in the network is

$$SR = \begin{bmatrix} r_{1,1}, & r_{1,2}, & \cdots, & r_{1,J} \\ r_{2,1}, & r_{2,2}, & \cdots, & r_{2,J} \\ \vdots & \vdots & \ddots & \vdots \\ r_{J,1}, & r_{J,2}, & \cdots, & r_{J,J} \end{bmatrix}$$
$$r_{j,j'} \in [0, 1], \quad \forall j, j' \in \mathcal{J}. \tag{2}$$

Here, mobile users are friends only when the social relation degree of two mobile users is greater than zero. Then, we have

$$f_{j,j'} = \begin{cases} 1, & if\ r_{j,j'} > 0 \\ 0, & otherwise \end{cases}, \quad \forall j, j' \in \mathcal{J}. \tag{3}$$

Here, $f_{j,j'}$ denotes whether mobile user j and mobile user j' are friends or not. Then, the number of mobile user j's friends can be calculated by

$$N_j = \sum_{j'=1, j' \neq j}^{J} f_{j,j'}, \quad \forall j, j' \in \mathcal{J}. \tag{4}$$

B. CONTENT MODEL

In the network, mobile users are desired to fetch contents from content providers. However, the content providers are usually deployed at remote area away from the users, inducing that it takes a long time to deliver one content. Therefore, mobile users hope that his/her desired contents can be cached on the nearby locations to reduce the retrieve latencies. In the network, with the edge computing, the contents can be cached on the edge nodes. If the caching capacity of an edge node is enough, the whole content of one user can be stored on this edge node. Otherwise, the edge node can store a part of the content and the rest part is stored on the content provider. Although only a part of content is stored in the content provider, the retrieve of this content is fast and the delivery latency for this part of content data can be reduced. Let $\mathcal{M} = \{1, 2, \cdots, m, \cdots, M\}$ denote the set of contents in the network.

Furthermore, the popularity of different contents should be considered. If a content with high popularity is cached on the edge node, there will be large number of requests and mobile users' QoE is also improved. The popularity of contents is characterized by a Zipf distribution. Here, the contents are sorted with the descending order of accessing times during a certain period (e.g., one day or one week, etc.). Namely, the accessing times of content 1 are larger than that of content 2. The popularity of content m, $(m \in \mathcal{M})$ can be quantified as

$$f_m = \frac{(\frac{1}{\tau(m)})^{\gamma}}{\sum_{m=1}^{M} (\frac{1}{m})^{\gamma}}, \tag{5}$$

where γ is a positive value to govern the skewness of the popularity. The popularity is uniformly distributed when $\gamma = 0$. Meanwhile, if γ is large, the popular contents account for the majority of requests from mobile users. $\tau(m)$ is the index of content m with the decreasing order of accessing times among all contents in the network. Specifically, the content m with small $\tau(m)$ has a large popularity. Indeed, the content popularity also implies the probability of requesting a content. If the popularity of content m is high, the probability that a user requests for content m is also large.

C. TRUST MODEL

Trust is a critical determinant for content sharing and social relationship. It is based on the reputations among individuals and is a capital asset that people may invest a great amount of resources. A user's trust on an edge node depends on whether the edge node can provide desired services with a required level of quality. Let $t_{i,j}$ denote the trust degree of mobile user j on edge node i, where $t_{i,j} \in [0, 1]$. The high value of $t_{i,j}$ means that mobile user j trusts edge node i with a high degree.

IV. THE FRAMEWORK OF PROPOSED SCHEME

In this section, we introduce the proposed scheme including trust evaluation, joint content caching and bandwidth leasing for mobile users.

A. TRUST EVALUATION

Before caching content, each mobile user assesses the reliability of edge nodes around him/her to find a trustworthy edge node to cache the content. Therefore, we introduce a trust evaluation mechanism for mobile users to find the trustworthy edge nodes. The trust of each edge node includes two parts: direct trust and indirect trust.

1) DIRECT TRUST

The direct trust is based on the direct interactions between the content generator and the edge nodes, inferred from the rating on the security quality of edge node, the caching size, allocated bandwidth, and the occurring timestamp of each interaction.

Firstly, after the interaction between a mobile user and an edge node, the mobile user will provide a rating on the secure service quality of this edge node. If the edge node is secure and reliable, the rating will be high. Let $Ra_{i,j}^k$ denote the trust rating of the k^{th} interaction between mobile user j and edge node i, we have

$$Ra_{i,j}^k = \log_2(1 + \Upsilon_{i,j}^k), \tag{6}$$

where $\Upsilon_{i,j}^k$ is the caching service quality of edge node i for mobile user j at the k^{th} interaction. Here, $0 \leq \Upsilon_{i,j}^k \leq 1$. The distrust rating of the k^{th} interaction is denoted by $Dr_{i,j}^k$, which can be obtained by

$$Dr_{i,j}^k = 1 - Ra_{i,j}^k. \tag{7}$$

Secondly, the caching sizes and prices in different interactions between mobile user j and edge node i during an interval $[0, \tau]$ are different. The rating of the service with the large caching size and bandwidth has a high effect on the derivation of direct trust. Let $s_{i,j}^k$ and $q_{i,j}^k$ denote the caching size and bandwidth provided by edge node i for mobile user j in the k^{th} interaction, respectively.

Thirdly, the rating of an edge node decays over time. Here, we consider an exponential decay function, which is

$$\tilde{\Lambda} = e^{-\varphi(\tau - \tau_k)}, \tag{8}$$

where $\varphi \in [0, \infty)$ and τ_k is the k^{th} interaction timestamp.

Therefore, we have the positive satisfaction experience as follows

$$PS_{i,j}(\tau) = \sum_{k=1}^{T_{i,j}(\tau)} W_{i,j}^k Ra_{i,j}^k e^{-\varphi(\tau - \tau_k)} \tag{9}$$

$$W_{i,j}^k = \frac{s_{i,j}^k q_{i,j}^k}{\sum_{k=1}^{T_{i,j}(\tau)} s_{i,j}^k q_{i,j}^k}, \tag{10}$$

where $T_{i,j}(\tau)$ is the interaction times between mobile user j and edge node i from the initial time to time τ. Similarly, the negative satisfaction experience is

$$NS_{i,j}(\tau) = \sum_{k=1}^{T_{i,j}(\tau)} W_{i,j}^k Dr_{i,j}^k e^{-\varphi(\tau - \tau_k)}. \tag{11}$$

In order to punish malicious behaviors, a punishment factor δ for negative satisfaction experience, which is a real number greater than 1, is introduced. Therefore, the direct trust can be expressed by

$$DT_{i,j}(\tau) = \frac{PS_{i,j}(\tau)}{PS_{i,j}(\tau) + \delta NS_{i,j}(\tau)}. \tag{12}$$

2) INDIRECT TRUST

Indirect trust is referred as recommendations from other mobile users on an edge node. Recommendations from other mobile users increase the trust evaluation accuracy, especially when a mobile user has no or very little experience with the given edge nodes. In such scenario, a mobile user requests other mobile users to provide the suggestions about the target edge node.

Honest mobile users always provide true recommendations, while malicious users may give false suggestions to conduct attacks. Consequently, recommendation credibility is needed to determine the reliability of a recommendation. During the indirect trust evaluation, recommendations provided by mobile users with high credibility are trustworthy. Here, every two mobile users have a certain similarity. If two mobile users have stronger similarity, the recommendations of them are more trustworthy. Thus the similarity can be used to describe the credibility. The similarity of two mobile users includes social similarity and rating similarity.

The social similarity can be divided into friendship similarity, visit similarity, and access similarity. The friendship similarity means the intimacy between two mobile users. Namely, the friendship similarity can be calculated based on the number of same friends. After two mobile users exchange their friend set, F_j and $F_{j'}$, they could compute two binary vectors, $\overrightarrow{VF_j}$ and $\overrightarrow{VF_{j'}}$, each with size $|F_j \bigcup F_{j'}|$. An element in $\overrightarrow{VF_j}$ (or $\overrightarrow{VF_{j'}}$) will be 1 if the corresponding user is in F_j (or $F_{j'}$), and otherwise 0. Then, the friendship similarity can be calculated by

$$\widehat{F}_{j,j'} = \frac{\overrightarrow{VF_j} \cdot \overrightarrow{VF_{j'}}}{||\overrightarrow{VF_j}|| \cdot ||\overrightarrow{VF_{j'}}||}. \tag{13}$$

The visit similarity means the closeness, which is an indication to show whether two nodes have the same physical contacts. The operational area of the network could be partitioned into sub-grids. Each mobile user records the IDs of sub-grid that he/she visits. Let P_j and P_j' denote the sets of the visited sub-grids of mobile user j and mobile user j', respectively. Therefore, the visit similarity can be obtained by

$$\widehat{V}_{j,j'} = \frac{\overrightarrow{VP_j} \cdot \overrightarrow{VP_{j'}}}{||\overrightarrow{VP_j}|| \cdot ||\overrightarrow{VP_{j'}}||}, \tag{14}$$

where $\overrightarrow{VP_j}$ and $\overrightarrow{VP_{j'}}$ are the position vectors of mobile user j and mobile user j', respectively, with size $|P_j \bigcup P_{j'}|$. Access similarity is based on the number of the same edge nodes that mobile users connect. If two mobile users have high access similarity, they are likely to have the common knowledge on edge nodes. Let D_j and $D_{j'}$ denote the sets of accessed edge nodes of mobile user j and mobile user j', respectively. The access similarity can be obtained by

$$\widehat{A}_{j,j'} = \frac{\overrightarrow{VD_j} \cdot \overrightarrow{VD_{j'}}}{||\overrightarrow{VD_j}|| \cdot ||\overrightarrow{VD_{j'}}||}, \tag{15}$$

where $\overrightarrow{VD_j}$ and $\overrightarrow{VD_{j'}}$ are the access vectors of mobile user j and mobile user j', respectively. Therefore, the social similarity can be obtained by

$$\mathfrak{S}_{j,j'} = w_f \cdot \widehat{F}_{i,j} + w_v \cdot \widehat{V}_{i,j} + w_a \cdot \widehat{A}_{i,j}, \tag{16}$$

where w_f, w_v, and w_a are weighted parameters.

The rating similarity is based on the ratings on the same edge nodes from two mobile users, which can be obtained by

$$\mathfrak{R}_{j,j'} = \frac{\sum_{i=1}^{I} (DT_{i,j} \times DT_{i,j'})}{\sqrt{\sum_{i=1}^{I} (DT_{i,j})^2} \times \sqrt{\sum_{i=1}^{I} (DT_{i,j'})^2}}. \tag{17}$$

Therefore, by combining the social similarity and rating similarity, the similarity between mobile user j and j' can be calculated by

$$\mathbb{S}_{j,j'} = \zeta \mathfrak{R}_{j,j'} + (1-\zeta)\mathfrak{S}_{j,j'}, \tag{18}$$

where ζ is the weighted parameter.

The credibility degree of mobile user j' measured by mobile user j is defined as

$$Cre_{j,j'} = \frac{e^{r_{j,j'}} \cdot \mathbb{S}_{j,j'}}{\sum_{j'=1}^{J} e^{r_{j,j'}} \cdot \mathbb{S}_{j,j'}}. \tag{19}$$

With credibility degree of each mobile user, the indirect trust can be obtained by

$$IT_{i,j} = \sum_{j'=1}^{J} Cre_{j,j'} \cdot DT_{i,j'}. \tag{20}$$

The trust degree of edge node i from the mobile user j becomes

$$t_{i,j} = \mu DT_{i,j} + (1-\mu) IT_{i,j}, \tag{21}$$

where μ is the weight of direct trust, which can be calculated as follows

$$\mu = \frac{T_{i,j}(\tau)}{T_{i,j}(\tau) + \sum_{j'=1}^{J} Cre_{j,j'} T_{i,j'}(\tau)}. \tag{22}$$

After the trust evaluation on each edge node, the mobile user who wants to cache content will set a trust threshold tr to select the trustworthy edge node for content caching and bandwidth allocation.

B. JOINT BANDWIDTH AND CACHING RESOURCE ALLOCATION

When a mobile user wants to cache a content on the edge node, he/she hopes that the caching size and the allocated bandwidth are large and the price charged by the edge node is low. From the edge node's perspective, it wants to earn benefits with the price as high as possible. Obviously, there exist competitions among mobile users and edge nodes. Therefore, we use the reverse auction to model the interactions among mobile users and edge nodes.

Reverse auction game is used to select the optimal candidate for providing services or goods, where there is one buyer and multiple sellers. The buyer is the auctioneer to buy the goods and the sellers are bidders to be the winners. Different from the normal auction game, the bidders in reverse auction game not only determine the prices that the buyer should pay, but also decide the amount of resources provided to the buyer. Then, the buyer selects the bidder with the highest score as the winner, and pays the price determined by the winner. In this paper, the buyers are the mobile users and the bidders are referred to different edge nodes. Here, the mobile user who wants to cache contents should firstly broadcast the base demand to nearby edge nodes, and then each edge node will submit the optimal bid to the mobile user for maximizing its utility. This mobile user will select the optimal edge node who can maximize his/her utility. Specifically, given the bid of edge node i, the utility of mobile user j who desires to cache content m is denoted by

$$u^b_{i,j,m} = \Gamma(s_{i,j,m}, q_{i,j,m}) - p_{i,j,m}, \tag{23}$$

where $p_{i,j,m}$ is the price determined by edge node i. $\Gamma(s_{i,j,m}, q_{i,j,m})$ is the satisfactory function of mobile user j to cache the content m. Formally, $\Gamma(s_{i,j,m}, q_{i,j,m})$ can be calculated by

$$\begin{aligned}\Gamma(s_{i,j,m}, q_{i,j,m}) &= \alpha_{j,m}\log(1+\varepsilon_s + t_{i,j}f_m\rho_{i,m}(s_{i,j,m} - \underline{s}_{j,m})) \\ &\quad + (1-\alpha_{j,m})\log(1+\varepsilon_q + t_{i,j}f_m\rho_{i,m}(q_{i,j,m} - \underline{q}_{j,m})),\end{aligned} \tag{24}$$

where $\alpha_{j,m}$ is the weighted parameter. ε_s and ε_q are positive values to guarantee that $\Gamma(s_{i,j,m}, q_{i,j,m})$ is lager than zero. Namely, if both the caching size and bandwidth provided by the edge node i are equal to the base demands of mobile user j, the mobile user still has a ceratin positive satisfaction. $\underline{s}_{j,m}$ is the base demand of mobile user j on caching size for content m and $\underline{q}_{j,m}$ is the base demand on bandwidth of mobile user j for content m. Therefore, the utility of mobile user j can be rewritten as

$$\begin{aligned}u^b_{i,j,m} &= \alpha_{j,m}\log(1+\varepsilon_s + t_{i,j}f_m\rho_{i,m}(s_{i,j,m} - \underline{s}_{j,m})) \\ &\quad + (1-\alpha_{j,m})\log(1+\varepsilon_q + t_{i,j}f_m\rho_{i,m}(q_{i,j,m} - \underline{q}_{j,m})) \\ &\quad - p_{i,j,m}.\end{aligned} \tag{25}$$

The utility function of edge node i can be defined by

$$u^s_{i,j,m} = \beta_{i,j,m}(p_{i,j,m} - C_{i,j,m}(s_{i,j,m}, q_{i,j,m})). \tag{26}$$

Here, $\beta_{i,j,m}$ is a binary variable, where $\beta_{i,j,m} = 1$ if the edge node i is selected as the winner by mobile user j for content m and otherwise, $\beta_{i,j,m} = 0$. $C_{i,j,m}(s_{i,j,m}, q_{i,j,m})$ is the cost function of edge node i to cache content m for mobile user j. Since each edge node in the game is rational, its utility should be nonnegative, where we have

$$p_{i,j,m} \geq C_{i,j,m}(s_{i,j,m}, q_{i,j,m}). \tag{27}$$

The cost function can be defined by

$$C_{i,j,m}(s_{i,j,m}, q_{i,j,m}) = \varsigma_{i,j,m}\theta^c s_{i,j,m} + \varsigma_{i,j,m}\theta^b q_{i,j,m}, \tag{28}$$

where θ^c and θ^b are the fixed cost coefficients of caching resource and bandwidth, respectively. Both θ^c and θ^b are common knowledge to all edge nodes. $\varsigma_{i,j,m}$ is the cost parameter of edge node i for mobile user j to cache content m. Indeed, the detailed cost parameter of each edge node is private and cannot be known by other edge nodes. But each edge node can estimate the others' cost parameters by the uniform distribution as follows:

$$f(\varsigma_{i,j,m}) = \begin{cases} \dfrac{1}{\varsigma_{\max} - \varsigma_{\min}}, & \varsigma_{\min} \leq \varsigma_{i,j,m} \leq \varsigma_{\max} \\ 0, & otherwise, \end{cases} \tag{29}$$

where $\varsigma_{\min}$ and $\varsigma_{\max}$ are the minimum and the maximum cost parameters, respectively. Therefore, the utility of edge node i can be rewritten as

$$u^s_{i,j,m} = \beta_{i,j,m}(p_{i,j,m} - \varsigma_{i,j,m}\theta^c s_{i,j,m} - \varsigma_{i,j,m}\theta^b q_{i,j,m}). \tag{30}$$

After each edge node submits the bid to the mobile user, the mobile user selects the edge node that can provide the maximum benefit as the winner. Thus each edge node has a certain probability to win the game. Here the probability that edge node i wins the game is denoted by $\mathbb{P}_i$. Thus the expected utility of edge node i is

$$\begin{aligned}E\{u^s_{i,j,m}\} = \mathbb{P}_i \cdot (p_{i,j,m} - \varsigma_{i,j,m}\theta^c s_{i,j,m} - \varsigma_{i,j,m}\theta^b q_{i,j,m}) \\ \times (1-\mathbb{P}_i)\cdot 0.\end{aligned} \tag{31}$$

All edge nodes participating the auction have the same target to maximize their utilities. Based on these targets, each edge node determines the optimal bid including price, caching size, and bandwidth. Therefore, the optimization problem for edge node i can be described as

$$\begin{aligned}&\max\ E\{u^s_{i,j,m}\} \\ &s.t. \begin{cases} \underline{s}_{j,m} \leq s_{i,j,m} \leq \min\{s_m, s^r_i\} \\ \underline{q}_{j,m} \leq q_{i,j,m} \leq q^r_i \\ u^s_{i,j,m} \geq 0, \end{cases}\end{aligned} \tag{32}$$

where s_m is the data size of content m. s^r_i and q^r_i are the remaining caching space and bandwidth of edge node i, respectively.

To resolve this optimization problem, the optimal caching size and bandwidth for mobile user j to cache content m is calculated. The optimal price is determined by edge node i to charge mobile user j .

Theorem 1: The optimal bid of edge node i on the caching size and bandwidth for mobile user j to cache content m can be given by

$$\begin{aligned}{s_{i,j,m}}^* = \arg\max_{s_{i,j,m}} \{&\alpha_{j,m}\log(1+\varepsilon_s + t_{i,j}f_m\rho_{i,m}(s_{i,j,m} - \underline{s}_{j,m})) \\ &+ (1-\alpha_{j,m})log(1+\varepsilon_q + t_{i,j}f_m\rho_{i,m}(q_{i,j,m} - \underline{q}_{j,m}) \\ &- \varsigma_{i,j,m}\theta^c s_{i,j,m} - \varsigma_{i,j,m}\theta^b q_{i,j,m}\}\end{aligned} \tag{33}$$

$$\begin{aligned}{q_{i,j,m}}^* = \arg\max_{q_{i,j,m}}\{&\alpha_{j,m}\log(1+\varepsilon_s + t_{i,j}f_m\rho_{i,m}(s_{i,j,m} - \underline{s}_{j,m})) \\ &+ (1-\alpha_{j,m})log(1+\varepsilon_q + t_{i,j}f_m\rho_{i,m}(q_{i,j,m} - \underline{q}_{j,m}) \\ &- \varsigma_{i,j,m}\theta^c s_{i,j,m} - \varsigma_{i,j,m}\theta^b q_{i,j,m}\}.\end{aligned} \tag{34}$$

Proof: Firstly, it is assumed that the bid $(s_{i,j,m}{}^*, q_{i,j,m}{}^*)$ is not the optimal strategy of edge node i. Thus there exists another optimal bid $(p_{i,j,m}{}', s_{i,j,m}{}', q_{i,j,m}{}')$, which maximizes the utility of the edge node i. Here, $s_{i,j,m}{}' \neq s_{i,j,m}{}^*$, $q_{i,j,m}{}' \neq q_{i,j,m}{}^*$. Let

$$\begin{aligned} p_{i,j,m}{}^* = & \alpha_{j,m}\log(1+\varepsilon_s+t_{i,j}f_m\rho_{i,m}(s_{i,j,m}{}^*-\underline{s}_{j,m})) \\ & +(1-\alpha_{j,m})log(1+\varepsilon_q+t_{i,j}f_m\rho_{i,m}(q_{i,j,m}{}^*-\underline{q}_{j,m}) \\ & -\alpha_{j,m}\log(1+\varepsilon_s+t_{i,j}f_m\rho_{i,m}(s_{i,j,m}{}'-\underline{s}_{j,m})) \\ & -(1-\alpha_{j,m})log(1+\varepsilon_q+t_{i,j}f_m\rho_{i,m}(q_{i,j,m}{}'-\underline{q}_{j,m}) \\ & +p_{i,j,m}{}'. \end{aligned} \tag{35}$$

Therefore,

$$\begin{aligned} & p_{i,j,m}{}' - \varsigma_{i,j,m}\theta^c s_{i,j,m}{}' - \varsigma_{i,j,m}\theta^b q_{i,j,m}{}' \\ & = p_{i,j,m}{}^* - \alpha_{j,m}\log(1+\varepsilon_s+t_{i,j}f_m\rho_{i,m}(s_{i,j,m}{}^*-\underline{s}_{j,m})) \\ & \quad -(1-\alpha_{j,m})log(1+\varepsilon_q+t_{i,j}f_m\rho_{i,m}(q_{i,j,m}{}^*-\underline{q}_{j,m}) \\ & \quad +\alpha_{j,m}\log(1+\varepsilon_s+t_{i,j}f_m\rho_{i,m}(s_{i,j,m}{}'-\underline{s}_{j,m})) \\ & \quad +(1-\alpha_{j,m})log(1+\varepsilon_q+t_{i,j}f_m\rho_{i,m}(q_{i,j,m}{}'-\underline{q}_{j,m}) \\ & \quad -\varsigma_{i,j,m}\theta^c s_{i,j,m}{}' - \varsigma_{i,j,m}\theta^b q_{i,j,m}{}' \\ & \leq p_{i,j,m}{}^* - \alpha_{j,m}\log(1+\varepsilon_s+t_{i,j}f_m\rho_{i,m}(s_{i,j,m}{}^*-\underline{s}_{j,m})) \\ & \quad -(1-\alpha_{j,m})log(1+\varepsilon_q+t_{i,j}f_m\rho_{i,m}(q_{i,j,m}{}^*-\underline{q}_{j,m}) \\ & \quad +\alpha_{j,m}\log(1+\varepsilon_s+t_{i,j}f_m\rho_{i,m}(s_{i,j,m}{}^*-\underline{s}_{j,m})) \\ & \quad +(1-\alpha_{j,m})log(1+\varepsilon_q+t_{i,j}f_m\rho_{i,m}(q_{i,j,m}{}^*-\underline{q}_{j,m}) \\ & \quad -\varsigma_{i,j,m}\theta^c s_{i,j,m}{}^* - \varsigma_{i,j,m}\theta^b q_{i,j,m}{}^* \\ & = p_{i,j,m}{}^* - \varsigma_{i,j,m}\theta^c s_{i,j,m}{}^* - \varsigma_{i,j,m}\theta^b q_{i,j,m}{}^*. \end{aligned} \tag{36}$$

Obviously, Eq. (36) is contradictory to the initial assumption of the proof. Therefore, the bid $(s_{i,j,m}{}^*, q_{i,j,m}{}^*)$ is the optimal strategy on caching size and bandwidth. This completes our proof. ■

Then, according to Eq. (33) and Eq. (34), the optimal bid on caching size and bandwidth can be calculated by

$$s_{i,j,m}{}^* = \begin{cases} \underline{s}_{j,m}, \\ \quad \text{if } \dfrac{\alpha_{j,m}}{\varsigma_{i,j,m}\theta^c} - \dfrac{1+\varepsilon_s}{t_{i,j}f_m\rho_{i,m}} \leq 0 \\ \min\{s_m, S_i^r\}, \\ \quad \text{if } \dfrac{\alpha_{j,m}}{\varsigma_{i,j,m}\theta^c} - \dfrac{1+\varepsilon_s}{t_{i,j}f_m\rho_{i,m}} + \underline{s}_{j,m} \geq \min\{s_m, S_i^r\} \\ \dfrac{\alpha_{j,m}}{\varsigma_{i,j,m}\theta^c} - \dfrac{1+\varepsilon_s}{t_{i,j}f_m\rho_{i,m}} + \underline{s}_{j,m}, \\ \quad \text{otherwise} \end{cases} \tag{37}$$

$$q_{i,j,m}{}^* = \begin{cases} \underline{q}_{j,m}, & \text{if } \dfrac{1-\alpha_{j,m}}{\varsigma_{i,j,m}\theta^c} - \dfrac{1+\varepsilon_q}{t_{i,j}f_m\rho_{i,m}} \leq 0 \\ q_i^r, & \text{if } \dfrac{1-\alpha_{j,m}}{\varsigma_{i,j,m}\theta^c} - \dfrac{1+\varepsilon_q}{t_{i,j}f_m\rho_{i,m}} \geq q_i^r - \underline{q}_{j,m} \\ \dfrac{1-\alpha_{j,m}}{\varsigma_{i,j,m}\theta^c} - \dfrac{1+\varepsilon_q}{t_{i,j}f_m\rho_{i,m}} + \underline{q}_{j,m}, & \text{otherwise.} \end{cases} \tag{38}$$

Next, the optimal price in the bid to win the game is analyzed. Sine the optimal bid on caching size and bandwidth is obtained, the expected utility of the edge node i can be rewritten as

$$E\{u^s_{i,j,m}\} = \mathbb{P}_i \cdot \{\widetilde{u}^b_{i,j,m} - \widehat{u}^b_{i,j,m}\}, \tag{39}$$

where $\widetilde{u}^b_{i,j,m}$ is the maximum utility of the mobile user j provided by edge node i. We have

$$\begin{aligned} \widetilde{u}^b_{i,j,m} = & \alpha_{j,m}\log(1+\varepsilon_s+t_{i,j}f_m\rho_{i,m}(s_{i,j,m}{}^*-\underline{s}_{j,m})) \\ & +(1-\alpha_{j,m})log(1+\varepsilon_q+t_{i,j}f_m\rho_{i,m}(q_{i,j,m}{}^*-\underline{q}_{j,m}) \\ & -\varsigma_{i,j,m}\theta^c s_{i,j,m}{}^* - \varsigma_{i,j,m}\theta^b q_{i,j,m}{}^*. \end{aligned} \tag{40}$$

$\widehat{u}^b_{i,j,m}$ is the utility of the mobile user j with the bid $(p_{i,j,m}, s_{i,j,m}{}^*, q_{i,j,m}{}^*)$ of edge node i, which can be calculated by

$$\begin{aligned} \widehat{u}^b_{i,j,m} = & \alpha_{j,m}\log(1+\varepsilon_s+t_{i,j}f_m\rho_{i,m}(s_{i,j,m}{}^*-\underline{s}_{j,m})) \\ & +(1-\alpha_{j,m})log(1+\varepsilon_q+t_{i,j}f_m\rho_{i,m}(q_{i,j,m}{}^*-\underline{q}_{j,m}) \\ & -p_{i,j,m}. \end{aligned} \tag{41}$$

Note that the mobile user j wants to select an edge node that can provide the maximum utility. Namely, we can have

$$u^b_{i,j,m}{}^* = \max\{u^b_{i,j,m} | i = 1, 2, \cdots, I\}. \tag{42}$$

Therefore, each edge node intends to determine an optimal bid price in order to win the game. For edge node i, the bid strategy to win the auction by competing with other edge nodes is formulated by $\widehat{u}^b_{i,j,m} = \Psi_{i,j,m}(\widetilde{u}^b_{i,j,m})$. Since each edge node is rational, $\Psi_{i,j,m}(\cdot)$ is a monotonic increasing function. According to Eq. (42), edge node i can obtain benefit only when its bid can maximize mobile user's utility. Otherwise, the benefit of edge node i is zero. Thus the probability $\mathbb{P}_i$ also means that the bid of edge node i can maximize the utility of mobile user j. It can be obtained by

$$\mathbb{P}_i = \prod_{i'=1, i'\neq i}^{I} \Pr\{\widehat{u}^b_{i,j,m} > \widehat{u}^b_{i',j,m}\}. \tag{43}$$

Since $\widehat{u}^b_{i,j,m} = \Psi_{i,j,m}(\widetilde{u}^b_{i,j,m})$ and $\Psi_{i,j,m}(\cdot)$ is a monotonic increasing function, we can have

$$\Pr\{\widehat{u}^b_{i,j,m} > \widehat{u}^b_{i',j,m}\} = \Pr\{\widetilde{u}^b_{i,j,m} > \widetilde{u}^b_{i',j,m}\}. \tag{44}$$

As an edge node cannot have entire information on the bids of other edge nodes, $\widetilde{u}^b_{i',j,m}$ is the random variable for edge node i. Therefore, the probability distribution function of the bid for edge node i is

$$\begin{aligned} F(\widetilde{u}^b_{i,j,m}) &= \Pr\{\widetilde{u}^b_{i,j,m} > \widetilde{u}^b_{i',j,m}\} \\ &= \Pr\{\varsigma_{i,j,m} < \varsigma_{i',j,m}\} \\ &= 1 - \Omega(\varsigma_{i,j,m}), \end{aligned} \tag{45}$$

where $\Omega(\cdot)$ is the probability distribution function of the cost parameter of edge node i'. Therefore, the probability of P_i can be calculated by

$$\mathbb{P}_i = (F(\widetilde{u}^b_{i,j,m}))^{I-1} = (1-\Omega(\varsigma_{i,j,m}))^{I-1}. \tag{46}$$

In order to reflect the relation between the probability $\mathbb{P}_i$ and $\widehat{u}^b_{i,j,m}$, let $\mathbb{P}_i = H(\widetilde{u}^b_{i,j,m}) = H(\Psi^{-1}_{i,j,m}(\widehat{u}^b_{i,j,m}))$. Thus, the utility of edge node i can be rewritten as

$$E\{u^s_{i,j,m}\} = H(\Psi^{-1}_{i,j,m}(\widehat{u}^b_{i,j,m})) \cdot \{\widetilde{u}^b_{i,j,m} - \widehat{u}^b_{i,j,m}\}. \quad (47)$$

By taking the first derivative of $E\{u^s_{i,j,m}\}$ with respect to $\widehat{u}^b_{i,j,m}$, we have

$$\frac{\partial E\{u^s_{i,j,m}\}}{\partial \widehat{u}^b_{i,j,m}} = \frac{\dot{H}(\Psi^{-1}_{i,j,m}(\widehat{u}^b_{i,j,m})) \cdot \{\widetilde{u}^b_{i,j,m} - \widehat{u}^b_{i,j,m}\}}{\dot{\Psi}_{i,j,m}(\Psi^{-1}_{i,j,m}(\widehat{u}^b_{i,j,m}))} - H(\Psi^{-1}_{i,j,m}(\widehat{u}^b_{i,j,m})), \quad (48)$$

where $\dot{H}(\cdot)$ is the derivative of the $H(\cdot)$ with respect to $\widehat{u}^b_{i,j,m}$. In order to maximize $E\{u^s_{i,j,m}\}$, let $\frac{\partial E\{u^s_{i,j,m}\}}{\partial \widehat{u}^b_{i,j,m}} = 0$ and we can obtain

$$\frac{\partial[H(\widetilde{u}^b_{i,j,m})\Psi_{i,j,m}(\widetilde{u}^b_{i,j,m})]}{\partial \widetilde{u}^b_{i,j,m}} = \dot{H}(\widetilde{u}^b_{i,j,m})\widetilde{u}^b_{i,j,m}. \quad (49)$$

By solving Eq. (49), we have

$$\Psi_{i,j,m}(\widetilde{u}^b_{i,j,m}) = \frac{1}{H(\widetilde{u}^b_{i,j,m})}\int_0^{\widetilde{u}^b_{i,j,m}} \dot{H}(y)y dy = \widetilde{u}^b_{i,j,m} - \frac{1}{H(\widetilde{u}^b_{i,j,m})}\int_0^{\widetilde{u}^b_{i,j,m}} H(y)dy. \quad (50)$$

Therefore, the optimal strategy on price determined by edge node i can be obtained with

$$p_{i,j,m}{}^* = \varsigma_{i,j,m}\theta^c s_{i,j,m}{}^* + \varsigma_{i,j,m}\theta^b q_{i,j,m}{}^* + \frac{1}{H(\widetilde{u}^b_{i,j,m})}\int_0^{\widetilde{u}^b_{i,j,m}} H(y)dy. \quad (51)$$

Here, $H(\widetilde{u}^b_{i,j,m})$ can be calculated by

$$H(\widetilde{u}^b_{i,j,m}) = (1 - \Omega(\varsigma_{i,j,m}))^{I-1}. \quad (52)$$

With Eq. (51), the optimal bid price of edge node i can be calculated by

$$p_{i,j,m}{}^* = \varsigma_{i,j,m}\theta^c s_{i,j,m}{}^* + \varsigma_{i,j,m}\theta^b q_{i,j,m}{}^* + \frac{1}{(1-\Omega(\varsigma_{i,j,m}))^{I-1}} \times \int_{\varsigma_{i,j,m}}^{\varsigma^{\max}_{i,j,m}} (\theta^c s_{i,j,m}{}^* + \theta^b q_{i,j,m}{}^*)(1-\Omega(y))^{I-1} dy. \quad (53)$$

Since $\varsigma_{i,j,m}$ follows the uniform distribution, $\Omega(\varsigma_{i,j,m})$ is

$$\Omega(\varsigma_{i,j,m}) = \frac{\varsigma_{i,j,m} - \varsigma^{\min}_{i,j,m}}{\varsigma^{\max}_{i,j,m} - \varsigma^{\min}_{i,j,m}}. \quad (54)$$

Thus the optimal bid price of edge node i is

$$p_{i,j,m}{}^* = \varsigma_{i,j,m}\theta^c s_{i,j,m}{}^* + \varsigma_{i,j,m}\theta^b q_{i,j,m}{}^* + \frac{(\theta^c s_{i,j,m}{}^* + \theta^b q_{i,j,m}{}^*)}{I}(\varsigma^{\max}_{i,j,m} - \varsigma_{i,j,m}). \quad (55)$$

Therefore, there exists a Bayesian equilibrium of the auction, if each edge node follows the optimal strategy, where the equilibrium strategies can be expressed as $\mathcal{O} = \{o_1^*, o_2^*, \cdots, o_I^*\}$ and $o_i^* = (s_{i,j,m}{}^*, q_{i,j,m}{}^*, p_{i,j,m}{}^*)$.

By comparing the utilities of mobile user j with the bids of all proper candidate edge nodes, the optimal candidate edge node is chosen by

$$i^* = \arg\max_i u^b_{i,j,m}, \quad i \in \mathcal{I}. \quad (56)$$

V. PERFORMANCE EVALUATION

In this section, we conduct simulations to evaluate the performance of the proposed scheme for smart campus. The simulation setup is first introduced and then the numerical results are given.

A. SIMULATION SETUP

In the simulation scenario, there are 20 edge nodes and 50 mobile users. Initially, the ratio of malicious edge nodes, speculative edge nodes, and legitimate edge nodes are 0.2, 0.3, 0.5, respectively. The maximum bandwidth of each edge node follows a uniform distribution $[40, 60]Mb$. The caching capacity of each edge node is uniformly distributed in $[45, 55]Mb$. The social relationship degrees among mobile users are randomly determined between 0 and 1. Each mobile user desires to cache a content with a probability of 0.1 every 5 seconds. The data size of each content is randomly selected in $[5, 10]Mb$. The content lifetime is 100 seconds. The initial direct trust degree between a mobile user and an edge node is 0.5. The trust threshold is 0.35. The secure service quality of the legitimate node is uniformly distributed in [0.7, 1] and that of malicious edge node is randomly determined within [0, 0.3]. The rating given by a mobile user to an edge node is equal to the quality of service. The probability that a malicious edge node provides a low price is 0.7. The simulation time is 3000. Based on [34], other parameters have been concluded in Table 1.

TABLE 1. Parameters.

Parameter	Value
$\alpha_{j,m}$	0.5
θ^c	0.6
θ^q	0.4
$\underline{s}_{j,m}$	0
$\underline{q}_{j,m}$	0
ε_s	0
ε_q	0
ζ	0.7
w_f	0.33
w_v	0.33
w_a	0.34
$\varsigma^{\min}_{i,j,m}$	0.07
$\varsigma^{\max}_{i,j,m}$	0.13

This paper uses the following metrics to compare different joint caching and bandwidth leasing scheme:

- **Secure caching ratio:** The data size of contents that are cached on the legitimate edge nodes to the total content data size during simulation time.
- **Average saved time:** The average reduced retrieve delay of a content from edge nodes, compared to require contents from remote content servers.

B. NUMERICAL RESULTS

The proposed scheme is compared with two conventional caching schemes as below.

Random scheme [34]: In this scheme, each mobile user randomly selects a nearby edge node to cache content and the selected edge node also randomly allocates the caching size and bandwidth to this user.

Auction based scheme [35]: In this scheme, the edge nodes are selected based on the reverse auction game, but there is no trust evaluation mechanism to assess the reliability of each edge node.

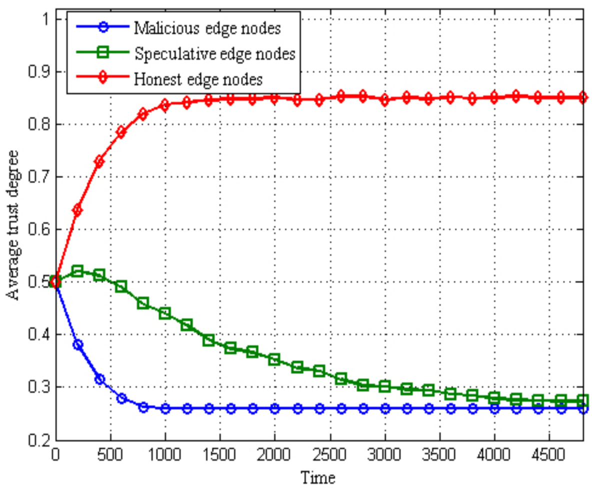


FIGURE 2. The evolution of averaged trust degree.

We first execute the simulation to analyze the trust degree of each edge node over time. In this simulation, service rating, cache size, bandwidth, price, and interaction timestamp between any edge node-user pair are known to all users. Fig. 2 shows the evolution of average trust degree for malicious edge nodes, speculative edge nodes, and legitimate edge nodes, respectively. The simulation time is 5000. Firstly, we can observe that the average trust degrees of malicious edge nodes and speculative edge nodes decrease over time, while the average trust degree of legitimate edge nodes increases. The reason is that legitimate edge nodes can provide the reliable and high quality of service and mobile users also give the positive trust rating on any legitimate edge node. In opposite, the quality of service given by the malicious edge node is low, with which the rating is also low. Besides, the decreasing rates of malicious edge nodes' average trust degrees are larger than speculative edge nodes. The reason is that the speculative edge node randomly selects its actions to be legitimate or malicious.

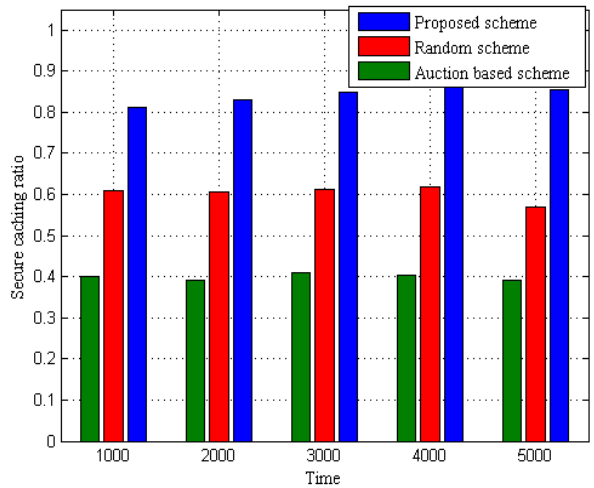


FIGURE 3. Secure caching ratio comparison between the proposal and other existing schemes, when the simulation time changes.

Fig. 3 is the comparison between the proposal and two conventional caching schemes on the secure caching ratio when the simulation time changes. Here, the simulation time is changed from 1000 to 5000. Other settings are unchanged. From Fig. 3, it can be observed that the proposal outperforms other schemes on the secure caching ratio at each simulation time. In the random scheme, the optimal edge nodes are randomly selected, where the selected optimal edge nodes may be malicious and don't securely cache contents. Even if the selected optimal edge nodes is speculative, it also has a probability to be malicious. In the auction based scheme, since there is no trust evaluation mechanism, malicious edge nodes have a high probability to provide low prices for defrauding mobile users to win the game.

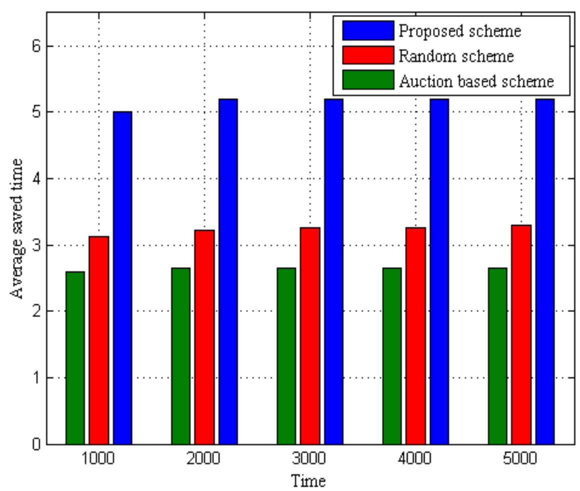


FIGURE 4. Average saved time comparison between the proposal and other existing schemes, when the ratio of honest edge nodes changes.

Fig. 4 shows the average saved time of the proposal compared with other two conventional schemes when the simulation time is changed from 1000 to 5000. From Fig. 4, we can see that the proposed scheme outperforms other schemes on the content delivery delay. In the random scheme, the caching size that the selected edge node provides for a content is randomly determined. Besides, the selected edge node may not be a cooperative legitimate edge node, and the content is not cached on the edge node. Thus the random scheme cannot significantly reduce content retrieval latency. In the auction based scheme, since there is no trust evaluation mechanism, the selected edge node may be malicious, inducing that mobile users have to obtain contents from remote content providers. In the proposed scheme, the optimal strategy on the caching size for a content is analyzed by the reverse auction game, where the mobile users can obtain the highest utilities. In addition, the trust degree guarantees that most of contents can be cached on the trustworthy edge nodes.

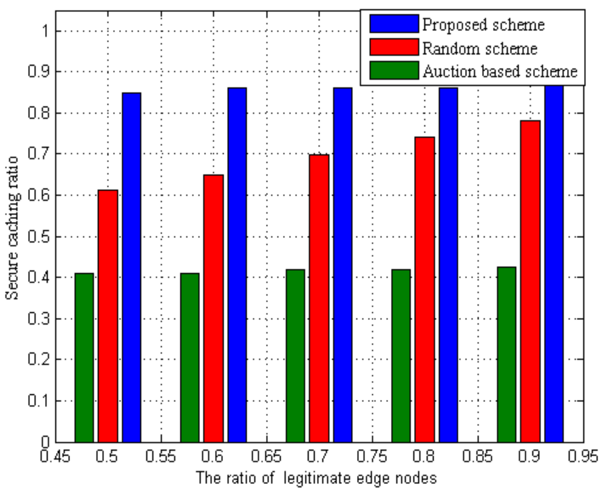


FIGURE 5. Secure caching ratio comparison between the proposal and other existing schemes, when the ratio of legitimate edge node changes.

Fig. 5 is the comparison between the proposal and other two conventional schemes on the secure caching ratio when the ratio of legitimate edge nodes changes. Here, the simulation time is 3000 and the ratio of legitimate edge nodes changes from 0.5 to 0.9. From Fig. 5, it can be shown that the proposed scheme has the highest secure caching ratio than other existing schemes. Especially, when the ratio of legitimate edge nodes is low, the proposed scheme has significant advantages. In addition, the secure caching ratio of each scheme gradually increases with the ratio of legitimate edge nodes. The reason is that more contents can be cached on the legitimate edge nodes that can provide reliable services for mobile users.

Fig. 6 shows the average saved time to retrieve contents with different schemes, where the ratio of legitimate edge nodes in the network changes from 0.5 to 0.9. The simulation time is 3000 and other settings are unchanged. In Fig. 6, the proposed scheme has the largest average saved time than other schemes. In the random scheme, mobile users randomly select the optimal edge nodes to cache contents, where the selected edge nodes may be malicious. In the auction based

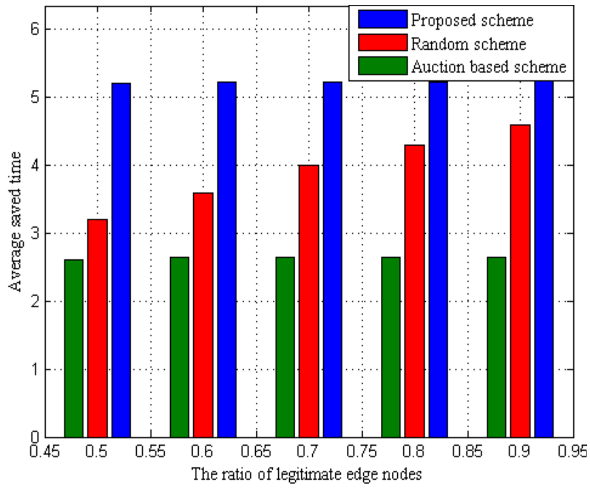


FIGURE 6. Average saved time comparison between the proposal and other existing schemes, when the ratio of legitimate edge node changes.

scheme, the optimal selected edge nodes may be malicious, where each malicious edge node fraudulently gives a low price to win the auction. In the proposed scheme, the optimal edge nodes are selected with auction game and trust evaluation mechanism, where contents can be securely cached and obtained from legitimate edge nodes. Therefore, the content retrieve delay with the proposed scheme is the minimum.

VI. CONCLUSION

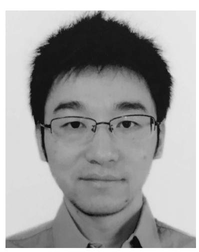
This paper has presented a reverse auction game based trustworthy edge caching and bandwidth allocation for multiple contents in MSNs for smart campus. We first introduce a trust evaluation mechanism to show the reliability of each edge node, where the trust degree of each edge node is analyzed by the direct trust and indirect trust. The direct trust is based on historical interactions while the indirect trust is determined by the recommendations from other mobile users. After evaluating the reliability of edge nodes, the reverse auction game is used to make the optimal decision for mobile users about selecting edge nodes. With the back induction method, the Bayesian equilibrium is obtained to provide the stable caching and bandwidth allocation scheme for mobile users. Finally, the simulations show that the proposed scheme can improve the mobile users' QoE and protect the network from the attacks of malicious edge nodes. About the future work, we will consider the privacy disclosure of mobile users when their contents are cached on the edge nodes.

REFERENCES

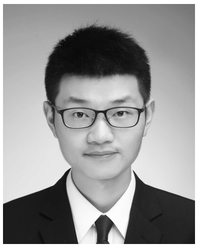
[1] A. Ndikumana, N. H. Tran, T. M. Ho, D. Niyato, Z. Han, and C. S. Hong, "Joint incentive mechanism for paid content caching and price based cache replacement policy in named data networking," *IEEE Access*, vol. 6, pp. 33702–33717, 2018.
[2] Z. Su, Y. Hui, Q. Xu, T. Yang, J. Liu, and Y. Jia, "An edge caching scheme to distribute content in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 5346–5356, Jun. 2018.
[3] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2869297.

[4] K. Zhang, K. Yang, X. Liang, Z. Su, X. Shen, and H. H. Luo, "Security and privacy for mobile healthcare networks: From a quality of protection perspective," *IEEE Wireless Commun.*, vol. 22, no. 4, pp. 104–112, Aug. 2015.
[5] Z. Su, Y. Hui, and T. H. Luan, "Distributed task allocation to enable collaborative autonomous driving with network softwarization," *IEEE J. Sel. Areas Commun.*, to be published, doi: 10.1109/JSAC.2018.2869948.
[6] H. Chen, Z. Su, Y. Hui, and H. Hui, "Dynamic charging optimization for mobile charging stations in Internet of Things," *IEEE Access*, to be published, doi: 10.1109/ACCESS.2018.2868937.
[7] *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021*, White Paper, 2017. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html
[8] K. Yang, K. Zhang, J. Ren, and X. Shen, "Security and privacy in mobile crowdsourcing networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 75–81, Aug. 2015.
[9] C. Zhu, J. J. P. C. Rodrigues, V. C. M. Leung, L. Shu, and L. T. Yang, "Trust-based communication for the industrial Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 16–22, Feb. 2018.
[10] Q. Xu and Z. Su, "Epidemic information spreading over mobile social networks with multiple social relationships," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–5.
[11] X. Liang, X. Li, K. Zhang, R. Lu, X. Lin, and X. S. Shen, "Fully anonymous profile matching in mobile social networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 641–655, Sep. 2013.
[12] N. Choudhury, R. Matam, M. Mukherjee, and L. Shu, "Beacon synchronization and duty-cycling in IEEE 802.15.4 cluster-tree networks: A review," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1765–1788, Jun. 2018.
[13] Z. Su, Q. Xu, J. Luo, H. Pu, Y. Peng, and R. Lu, "A secure content caching scheme for disaster backup in fog computing enabled mobile social networks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4579–4589, Oct. 2018.
[14] L. Hu, H. Wen, B. Wu, J. Tang, and F. Pan, "Adaptive base station cooperation for physical layer security in two-cell wireless networks," *IEEE Access*, vol. 4, pp. 5607–5623, 2016.
[15] Q. Xu, Z. Su, K. Zhang, P. Ren, and X. S. Shen, "Epidemic information dissemination in mobile social networks with opportunistic links," *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 3, pp. 399–409, Sep. 2015.
[16] Y.-J. Chang, H.-H. Liu, L.-D. Chou, Y.-W. Chen, and H.-Y. Shin, "A general architecture of mobile social network services," in *Proc. Int. Conf. Converg. Inf. Technol. (ICCIT)*, Nov. 2007, pp. 151–156.
[17] Y. Wang, J. Wu, and W.-S. Yang, "Cloud-based multicasting with feedback in mobile social networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6043–6053, Dec. 2013.
[18] R. Fei, K. Yang, and X. Cheng, "A cooperative social and vehicular network and its dynamic bandwidth allocation algorithms," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2011, pp. 63–67.
[19] Q. Xu, Z. Su, and M. Dai, "Trustworthy caching for mobile big data in social networks," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2018, pp. 808–812.
[20] C. Petrie, S. Gupta, V. Rao, and B. Nutter, "Energy efficient control methods of HVAC systems for smart campus," in *Proc. IEEE Green Technol. Conf. (GreenTech)*, Apr. 2018, pp. 133–136.
[21] Z. Tian *et al.*, "A real-time correlation of host-level events in cyber range service for smart campus," *IEEE Access*, vol. 6, pp. 35355–35364, 2018.
[22] A. Sivanathan *et al.*, "Characterizing and classifying IoT traffic in smart cities and campuses," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, May 2017, pp. 559–564.
[23] L. Wang, C. Yao, Y. Yang, and X. Yu, "Research on a dynamic virus propagation model to improve smart campus security," *IEEE Access*, vol. 6, pp. 20663–20672, 2018.
[24] L. Qiu, Q. Lei, and Z. Zhang, "Advanced sentiment classification of tibetan microblogs on smart campuses based on multi-feature fusion," *IEEE Access*, vol. 6, pp. 17896–17904, 2018.
[25] L. Liu and H. Jia, "Trust evaluation via large-scale complex service-oriented online social networks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 45, no. 11, pp. 1402–1412, Nov. 2015.
[26] J. Shen, T. Zhou, C.-F. Lai, J. Li, and X. Li, "Hierarchical trust level evaluation for pervasive social networking," *IEEE Access*, vol. 5, pp. 1178–1187, 2017.
[27] F. Hao, G. Min, M. Lin, C. Luo, and L. T. Yang, "MobiFuzzyTrust: An efficient fuzzy trust inference mechanism in mobile social networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 11, pp. 2944–2955, Nov. 2014.
[28] Y. Wang, "Trust quantification for networked cyber-physical systems," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2055–2070, Jun. 2018.
[29] L. Zhu, C. Zhang, C. Xu, and K. Sharif, "RTSense: Providing reliable trust-based crowdsensing services in CVCC," *IEEE Netw.*, vol. 32, no. 3, pp. 20–26, May/Jun. 2018.
[30] W. Zhi, K. Zhu, Y. Zhang, and L. Zhang, "Hierarchically social-aware incentivized caching for D2D communications," in *Proc. 22nd Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2016, pp. 316–323.
[31] X. Wang, S. Leng, and K. Yang, "Social-aware edge caching in fog radio access networks," *IEEE Access*, vol. 5, pp. 8492–8501, 2017.
[32] X. Zhang *et al.*, "Information caching strategy for cyber social computing based wireless networks," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 3, pp. 391–402, Jul./Sep. 2017.
[33] M. Taghizadeh, K. Micinski, C. Ofria, E. Torng, and S. Biswas, "Distributed cooperative caching in social wireless networks," *IEEE Trans. Mobile Comput.*, vol. 12, no. 6, pp. 1037–1053, Jun. 2013.
[34] Q. Xu, Z. Su, Q. Zheng, M. Luo, and B. Dong, "Secure content delivery with edge nodes to save caching resources for mobile users in green cities," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2550–2559, Jun. 2018.
[35] H. Zhou, K.-C. Leung, and V. O. K. Li, "Auction-based bandwidth allocation and scheduling in noncooperative wireless networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 2556–2561.

QICHAO XU is currently pursuing the Ph.D. degree with the School of Mechatronic Engineering and Automation, Shanghai University, Shanghai, China. His research interests are in the general area of wireless network architecture and vehicular networks.



ZHOU SU received the Ph.D. degree from Waseda University, Tokyo, Japan, in 2003. His research interests include multimedia communication, wireless communication, and network traffic. He is a TPC Member of some flagship conferences, including IEEE INFOCOM, IEEE ICC, IEEE Globecom, and so on. He received the Best Paper Award at the International Conference CHINACOM2008 and the Funai Information Technology Award for Young Researchers in 2009. He is the Chair of the Multimedia Services and Applications Over Emerging Networks Interest Group (MENIG) of the IEEE Comsoc Society, the Multimedia Communications Technical Committee. He also served as the Co-Chair of several international conferences, including IEEE VTC Spring 2016, IEEE CCNC2011, and so on. He is an Associate Editor of *IET Communications* and IEICE Transactions on Communications.



YUNTAO WANG is currently pursuing the master's degree with the School of Mechatronic Engineering and Automation, Shanghai University, Shanghai, China. His research interests are in the general area of wireless network architecture and smart grid.

MINGHUI DAI is currently pursuing the Ph.D. degree with the School of Mechatronic Engineering and Automation, Shanghai University, Shanghai, China. His research interests are in the general area of wireless network architecture and crowdsensing.