A Secure Content Caching Scheme for Disaster Backup in Fog Computing Enabled Mobile Social Networks

Zhou Su, Qichao Xu, Jun Luo, Huayan Pu, Yan Peng, and Rongxing Lu

***Abstract*—Caching content with fog computing at the edge nodes has been a promising alternative to mitigate burdens of backbone networks and improve mobile users' quality of experience in mobile social networks (MSNs). However, as edge node may be vulnerable due to the attacks from malicious users, the design of secure caching schemes for the fog/edge enabled MSNs becomes a new challenge. In this paper, to tackle the above problem, we propose a secure caching scheme for disaster backup in MSNs with fog computing. Specifically, to protect the privacy, a partitioning and scrambling method is first designed to encrypt the contents. Then, the encrypted contents are replicated to multiple replicates, where these replicates are delivered and stored in different servers. Based on the recovery time objective and content delivery latency, an auction game model is developed to determine the optimal servers, where both edge nodes and cloud servers can obtain the maximum utilities. Extensive simulations are conducted to show the effectiveness and reliability of the proposed scheme.**

***Index Terms*—Cloud server, content caching, disaster backup, mobile social networks (MSNs).**

I. Introduction

CONTENT delivery over mobile social networks (MSNs) has emerged as a promising alternative for mobile users to exchange and share contents with each other [1], [2]. Recent studies have shown that the total number of mobile devices connected to the Internet has been more than the population in the world since 2014. As the dramatic growth of mobile users has triggered an exponential increase of mobile data traffic [3], the backhaul link-capacity requirement to support mobile data becomes enormously high, where the delay to deliver vast contents among mobile users in core network needs to be resolved [4]–[10].

Fog/edge caching has been advocated to deliver contents for mitigating the backhaul link capacity requirement and reducing the latency to deliver content in MSNs [11]–[14]. The advantages of edge caching are threefold. First, popular contents can be cached on the edge nodes that are close to mobile users, so as to reduce the delay and improve mobile users' quality of experience (QoE). Second, redundant data transmissions over backhaul link in core network can also be significantly alleviated. Third, the majority of data traffic can be offloaded from the overloaded base stations to edge nodes.

Despite of the above advantages, the existing edge caching methods should be further optimized to cache contents in MSNs. On one hand, edge nodes may suffer from the attacks by malicious users or adversaries. For example, some mobile users are honest to store and deliver contents with edge nodes, while others may be malicious to spread the virus to edge nodes. On the other hand, some disasters including internal disasters and external disasters may happen to cause the lost of content at the edge nodes. For instance, when the operating system of the edge node stops working, some critical and important data may be removed or tampered. Besides, the breakout of natural disasters, such as fire, earthquake, etc., can make the power failure of edge nodes, where the cached contents of mobile users may be lost. Therefore, a secure caching scheme for edge nodes is needed to provide desired services for mobile users in MSNs.

To address the above challenges, the disaster backup is introduced based on the thought of redundancy, where the contents are replicated on multiple storages at different sites. Then, even though the cached contents on edge node are lost, the edge node still can retrieve these contents from remote sites. In addition, the edge node can also use the replicated contents in the remote sites to check the validity of contents cached on the edge nodes. For example, if an edge node suspects that the cached contents are tampered by malicious users, it can request the replicated contents from the remote cloud servers and compare the cached contents with the retrieved replicates to verify the effectiveness of cached contents. The recovery time objective (RTO) is an important parameter to show the time duration between the disruption and the restoration of service. By minimizing the RTO,

Manuscript received January 26, 2018; revised April 24, 2018; accepted June 3, 2018. Date of publication June 25, 2018; date of current version October 3, 2018. This work was supported in part by the NSFC under Grant 91746114, Grant 61571286, and Grant 61525305, in part by the Shanghai Key Laboratory of Power Station Automation Technology, in part by the NSERC Discovery Grants under Grant 04009, in part by the NBIF Start-Up Grant under Grant Rif 2017-012, in part by the HMF2017 YS-04, and in part by the NF-2017-05. Paper no. TII-18-0211. *(Corresponding author: Zhou Su and Jun Luo.)*

Z. Su, Q. Xu, J. Luo, H. Pu, and Y. Peng are with the School of Mechatronic Engineering and Automation, Shanghai University, Shanghai 200444, China (e-mail: zhousu@ieee.org; xqc690926910@shu.edu.cn; luojun@shu.edu.cn; phygood_2001@shu.edu.cn; pengyan@shu.edu.cn).

R. Lu is with School of Computer Science, University of New Brunswick, NB E3B 5A3, Canada (e-mail: rlu1@unb.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2018.2849984

the disaster backup can efficiently resume the service online after a disruption.

Recently, many efforts have been made for the disaster backup to improve the content caching performance in wireless communication networks [15]–[23]. But, most of the current approaches focus on how to store contents in cloud servers, where the privacy of content is not mainly considered. In addition, although the storage of edge nodes can be improved by storing content copies in cloud servers, most of works do not discuss the scenarios that the cloud server may be attacked by malicious users. Furthermore, how to select the optimal cloud servers still have not been investigated sufficiently. Therefore, it is still an open and vital issue to design a novel secure caching scheme for mobile users in MSNs.

In this paper, we present a disaster-backup-based secure caching scheme in MSNs for mobile users. First, in order to guarantee privacy of mobile users, a novel partitioning and scrambling method is designed to encrypt content without adding extra information and increasing the content size. Second, to realize the integrality of content, the encrypted content is replicated to multiple copies, which are delivered and stored in different cloud servers. Then, according to the security level of mobile users, the selection index is determined based on the RTO of each cloud server and the content delivery latency. With an auction game, the optimal cloud servers are determined, where both the edge nodes and cloud servers can obtain the maximum utilities. Extensive simulations are conducted to show the effectiveness and reliability of the proposed scheme. Specifically, the main contributions of our paper are threefold.

1) *Content encryption framework:* We propose a novel content encryption method to guarantee the privacy of mobile users. The content is first partitioned into multiple fragments, and then these fragments are scrambled without the change of content size and the loss of content information.
2) *Auction game-based cloud servers selection:* We introduce the auction game to model the selection of optimal cloud servers. The optimal price of cloud server can be obtained by a bid to win the auction game for maximizing both the utilities of edge nodes and cloud servers.
3) *Performance evaluation:* The performance of the proposed scheme is evaluated with extensive simulations. The simulation results show that the proposed scheme can obtain a higher security to price ratio and a better utility of the edge node than the conventional schemes on secure content caching for disaster backup.

The remainder of this paper is organized as follows. Section II recalls some related works. Section III presents the system model. Section IV introduces the proposed disaster-backup-based secure caching scheme. Section V evaluates the proposed scheme with extensive simulations and Section VI closes this work with conclusions.

II. Related Work

In this section, we review the related works, including content delivery in MSNs, content caching in wireless networks, and secure content storage with disaster backup.

A. Content Delivery in Mobile Social Networks

Hu *et al.* [24] provided a comprehensive survey with regard to features, platforms, architecture designs, and key technologies by comparing the MSNs with conventional social networks. Su *et al.* [25] proposed the framework for caching layered videos in the edge nodes based on the caching price, the available capacity of cache nodes, and the social features of mobile users. Li *et al.* [26] introduced a new architecture with multiple location servers to protect the privacy against the insider attack launched by the service providers. Abbas *et al.* [27] presented an efficient privacy protection and interests sharing protocol, which enables mobile users to discover mutual interests without revealing their interests. Xu *et al.* [28] improved content delivery by the optimization of peer discovery and resource allocation by combining the social and physical layer information in D2D underlay networks, where the social relationship is used as the weight to describe the impact of social features and content sharing. Ning *et al.* [29] presented an incentive data dissemination scheme in autonomous MSNs with two-person cooperative game-based data pulling model and online auction game-based data pushing model. However, the secure caching of content in MSNs is still not discussed sufficiently.

B. Content Caching in Wireless Networks

Liang *et al.* [30] presented the framework for QoE-aware wireless edge caching with bandwidth provisioning in software-defined wireless networks to improve the quality of QoE in caching. Xu *et al.* [31] formulated a stackelberg game and a radio resource-allocation-based algorithm for the adaptive bitrate video delivery to improve both the cache hit ratio and the system throughput. Zhou *et al.* [32] designed an stochastic optimization-based dynamic multicast scheduling scheme in cache-enabled content-centric wireless networks to minimize the average delay and fetching costs. Li *et al.* [33] deployed the collaborative multitier caching method, where the duplicated transmissions of content downloads are reduced and the network capacity are improved. Song *et al.* [34] explored the content caching problem with a multiarmed bandit learning algorithm to jointly optimize content popularity distributions and the cost of content retrieving. Malak *et al.* [35] proposed a spatially correlated content caching scheme for D2D networks, where each contents popularity follows the Zipf distribution and the locations of mobile users are modeled by the Poisson point process with limited communication range. Although most of works have studied the content caching in wireless networks, few of them focus on the secure content delivery.

C. Secure Content Storage With Disaster Backup

Chen *et al.* [36] proposed a secure cloud storage protocol to support both user anonymity and the third-party public auditing. Tian *et al.* [37] presented a novel public auditing scheme for secure cloud storage based on dynamic hash table, by combining the homomorphic authenticator. Tang *et al.* [38] designed a secure overlay cloud storage system that achieves fine-grained, policy-based access control, and file assured deletion. Yu *et al.* [39] proposed a paradigm named strong key-exposure resilient

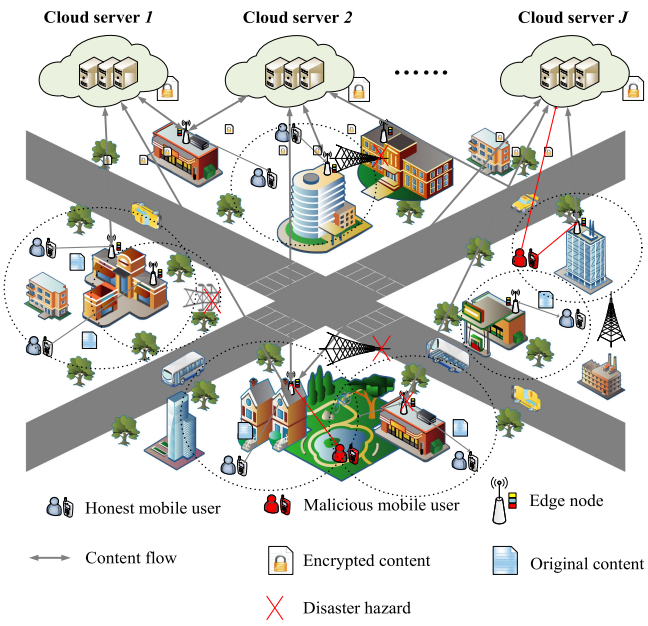


Fig. 1. System model.

auditing for secure cloud storage by formalizing the definition and the security model. Lin *et al.* [40] proposed a threshold proxy reencryption scheme and integrated it with a decentralized erasure code to support the secure and robust data storage. Li *et al.* [41] designed a novel receiving-capacity-constrained rapid and fair disaster backup strategy in the software defined network by guaranteeing upper bound of bandwidth allocation to achieve fair load distribution for backup datacenters. Xie *et al.* [42] solved the problem of emergency backup in interdatacenter networks with progressive disasters, where the time-expanded network approach is used to model the time-variant interdatacenter network during a progressive disaster. Although most of works have discussed how to securely content store using disaster backup, the privacy, and integrality of stored content are not sufficiently considered to against the attack by malicious users.

III. System Model

In this section, we introduce our system model including network model and content model, as shown in Fig. 1.

A. Network Model

1) *Cloud servers:* The network consists of multiple cloud servers which are enabled to provide power for computing and storage toward the disaster backup services. The local resource of mobile users can be saved when the contents are delivered and processed in cloud servers. The main goal of backup services is to resume contents online after a disruption. RTO is an important parameter which is used to evaluate performances of disaster backup services. RTO is defined by the time duration between the disruption until scheduling and restorations of contents. Let $\mathcal{J} = \{1, 2, \ldots, J\}$ denote the set of clouds in the network where these clouds can be accessed by all mobile users. Since each cloud is usually located in the remote area, it brings the latency for a mobile user to obtain contents from the remote cloud servers. Here, we assume that it needs l_j route nodes in core network to fetch the contents from cloud j. The bandwidth between two route nodes in the backbone network is b. Then, the delay to obtain the content of unit size is

$$d = \frac{1}{b}(l_j - 1) + \frac{1}{b_j} \tag{1}$$

where the bandwidth between cloud server i and core network is b_j.

2) *Edge nodes:* There exist multiple edge nodes in the system between cloud servers and mobile users. The edge node equipped with edge computing is an Internet-connected computer or server which is located at the edge of the cloud servers' backbone. Compared to the cloud servers, the edge node is much closer to mobile users. Therefore, the edge node can cache contents for mobile users with a short latency. In addition, the edge node can send the cached contents to remote cloud server for storage and backup. Let $\mathcal{I} = \{1, 2, \ldots, I\}$ denote the set of edge nodes in the network. When a group of edge nodes cooperatively provide contents for mobile users, these edge nodes can be seen as a coalition. In the coalition, the caching service for mobile users is available when the edge node with the largest RTO is restored.

3) *Mobile users:* In an MSN, if a mobile user has generated an interesting content, the user can cache the content on the edge node and recommend this content to his/her friends with a link via some social platforms (e.g., Facebook, Wechat), as the mobile users with social relationships usually have the similar interests. Thus, mobile users are willing to access the contents shared by their friends. Let $\mathcal{K} = \{1, 2, \ldots, K\}$ be the set of mobile users in the network. For any two mobile users, the social relationship degree is denoted as $r_{k,k'}, k, k' \in \mathcal{K}$, where $r_{k,k'} \in \{0, 1\}$. Here, $r_{k,k'} = 1$ means two mobile users k and k' have the social relationship, while $r_{k,k'} = 0$ means two mobile users k and k' have no relationship.

B. Content Model

A constant bit rate streaming content model is used to describe cached content, as an adaptive one to support mobile devices with different features to generate contents. The source file of content consists of multiple segments to be delivered to mobile users. Each segment is corresponding to a short playback time (e.g., 1–10 s) of the content, where users can download the content segment by segment. $\tilde{l}_k$ denotes the segment length of mobile user k's content. The bit rate of the content generated by mobile user k is denoted as bt_k. If a content of mobile user k has L_k seconds, the size of this content can be calculated by

$$D_k = L_k \cdot bt_k. \tag{2}$$

We further consider the popularity of different contents by a Zipf distribution. With the descending order of accessing times

during a certain period (e.g., one day or one week), the popularity of mobile user k's content is

$$f(m_k) = \frac{\left(\frac{1}{\hat{\tau}(m_k)}\right)^{\gamma}}{\sum_{k=1}^{K}\left(\frac{1}{\hat{\tau}(m_k)}\right)^{\gamma}} \tag{3}$$

where γ is the positive value to govern the skewness of the popularity. $\hat{\tau}(m_k)$ is the index of mobile user k's content with the decreasing order of accessing times among all contents stored on the cache nodes. Indeed, the popularity distribution indicates the request probabilities of different contents.

On one hand, as the storage resources in fog computing enabled MSNs can be shared by a group of cloud servers, if a cloud server is overloaded by a large number of contents, this cloud server can request for more storage to increase its caching resource. The cloud servers with a relative low number of contents can decrease its caching resource by removing some storage, which can be used by others. On the other hand, the cloud servers can cooperatively backup contents for edge nodes. The cloud server with a high burden can make a coalition with other cloud servers to request them to undertake a part of backup services. With the coalition to provide backup service, the caching resource utilization rate can be increased and the resource balancing is also achieved. If the content requester has a high security on content, the number of fragments divided from original content should be large to guarantee the privacy. The edge computing server can select the disaster backup services from cloud servers. Cloud servers are usually deployed at the remote area and can communicate with multiple edge nodes through the backbone networks.

IV. Disaster-Backup-Based Secure Caching Scheme

In this section, we first present the disaster backup method to guarantee the security of cached contents on the cached nodes, and then introduce the auction game-based optimal cloud servers selection.

A. Disaster Backup-Based Encryption Method

The disaster backup is introduced to resolve the security problem for cached contents on edge nodes. The disaster backup means that a system can be recovered after a disaster, since the functions and key data are conducted by backup in previous. Indeed, the backup employs the redundancy technology to improve the reliability of the system. The redundancy means the system becomes complicated by artificially increasing the repetition parts.

In order to guarantee the security of the cached content on the edge nodes, once the content is lost on the edge nodes, these edge nodes can retrieve this content from remote cloud servers to satisfy mobile users' demands. However, due to the unsafety of the cloud server, the disaster backup mechanism may bring two problems. On one hand, the privacy of the content may be broken, where some users' important information may be disclosed to edge nodes or malicious users, such as preferences, ages, sex, etc. On the other hand, the remote cloud servers may be attacked by some malicious users, where the integrality of the content may not be guaranteed.

To resolve the first problem, a content partitioning and scrambling method is designed to protect the privacy of the content. Since the contents on the edge node are integrated with different bitrates, the sizes of contents with the same time length are also different. Thereby, the size required by the remote cloud server is large to store the large sized content. To save the storage size, the edge nodes will transform the content to the one with the minimum bitrate. Therefore, the content size of mobile user k's content cached on edge node i will be transformed by

$$D_{i,k} = bt_{\min,i} \cdot L_{i,k} \tag{4}$$

where $L_{i,k}$ is the time length of mobile user k's content cached on edge node i. $bt_{\min,i}$ is the minimum bitrate determined by edge node i. Accordingly, although the content size of the content is reduced, the basic information is still stored. Next, the content is divided into fragments with a parameter $s_{i,k}$ which is the number of segments. Here, a fragment is combined by multiple segments. As a result, the total number of fragments for this content becomes

$$S_{i,k} = \left\lceil \frac{D_{i,k}}{s_{i,k} \cdot \tilde{l}_{i,k} \cdot bt_{\min,i}} \right\rceil \tag{5}$$

where $\lceil \cdot \rceil$ denotes ceiling function. And the number of bytes in one fragment can be calculated by

$$M_{i,k} = \frac{s_{i,k} \cdot \tilde{l}_{i,k} \cdot bt_{\min,i}}{8} \tag{6}$$

where $\tilde{l}_{i,k}$ is time length of the segment.

According to the content partitioning, the original content can form a matrix with the size of $S_{i,k} \times M_{i,k}$, where $S_{i,k}$ is the number of rows and $M_{i,k}$ is the number of columns. Each element of the matrix is a byte of original content. Initially, bytes are placed based on the orders of original content. Namely, $(a_{11}^{i,k}, a_{12}^{i,k}, \ldots, a_{1M_{i,k}}^{i,k})$ is the first fragment of the original content and bytes are arranged by the order of the divided fragment. Here, the orders of bytes are denoted as $TN_1 = \{\hat{p}_{11}, \hat{p}_{12}, \ldots, \hat{p}_{1M_{i,k}}\}$. Then, we use chaos map to scramble the orders of the bytes. The classical chaos system in one-dimension is a logistic map, which can be defined by the following [44]:

$$x(t+1) = \mu x(t)(1 - x(t)). \tag{7}$$

Here, $0 \le \mu \le 4$ is called a chaos parameter and $x(t) \in (0, 1)$. From chaos dynamic system, the logistic map becomes confusion if $3.569945... \le \mu \le 4$. That is to say, the chaos sequences $\{x(t)\}_{t=0}^{\infty}$ and $\{y(t)\}_{t=0}^{\infty}$ are nonperiodic, noncoverage, and pseudorandom, given by two different initial conditions $x(0)$ and $y(0)$. If $\mu = 4$, the chaos map of formula (7) has the best chaos effect. But this fixed value of μ will reduce a certain degree of security for the cached content. Thereby, we use a chaos sequence-based random function to represent the

parameter μ, where the new chaos function is

$$x(t+1) = \left[3.569945 + (4 - 3.569945) \cdot \sin\left(\frac{\pi}{2}x(t)\right)\right] \times x(t)(1 - x(t)). \quad (8)$$

And,

$$\tilde{\mu} = 3.569945 + (4 - 3.569945) \cdot \sin\left(\frac{\pi}{2}x(t)\right). \quad (9)$$

Here, the parameter $\tilde{\mu}$ of the new chaos function is not fixed and it varies at each iteration.

Given an initial value $x(0)$ and a positive integer n, a chaos sequence $\{x(t)\}_{t=0}^{\infty}$ can be obtained by formula (8). Then, for the generated sequence, we take $M_{i,k}$ values $\{x(n+1), x(n+2), \ldots, x(n+M_{i,k})\}$ out from the nth number. And, the ordering for this $M_{i,k}$ values can get $\{\overline{x}(n+1), \overline{x}(n+2), \ldots, \overline{x}(n+M_{i,k})\}$. Next, we find the position of values $\{\overline{x}(n+1), \overline{x}(n+2), \ldots, \overline{x}(n+M_{i,k})\}$ in $\{x(n+1), x(n+2), \ldots, x(n+M_{i,k})\}$ and mark down the transform positions $\mathrm{TM} = \{t_1, t_2, \ldots, t_{M_{i,k}}\}$. Therefore, the TM is the sequence vector that we want. In addition, we can transform the orders of bytes in the $\hat{n}$th row with TM. For transforming the next row, we set another initial value $y(0)$ to generate another chaos sequence $\{y(t)\}_{t=0}^{\infty}$. From this chaos sequence $\{y(t)\}_{t=0}^{\infty}$, a number is selected at random to generate the newly initial value of $x(0)$, which is

$$\tilde{x}(0) = \frac{x(0) + y(M_{i,k})}{2}. \quad (10)$$

With the similar step, the new row is scrambled. Also, we can get another value for the new $y(0)$ by computing

$$\tilde{y}(0) = \frac{y(0) + x(M_{i,k})}{2}. \quad (11)$$

After the rows are scrambled, we continue to scramble the columns, where the same process on each row will be done on each column. Based on the demand of security level for each edge node, we repeat this process by ϱ times. In addition, for each column or each row, we carry out the reversible operations for bytes, such as exclusive-or, binary addition, or binary subtraction.

To solve the second problem, i.e., the content may be lost or tampered, the scrambled contents are replicated by $\tilde{j}$ copies which are stored in different remote cloud severs. Therefore, the privacy and integrality of cached contents are preserved for mobile users. For details, a disaster-backup-based content encryption algorithm is given by Algorithm 1.

Algorithm 1: Disaster-Backup-Based Content Encryption Algorithm.

Input: The content length L_j, the content bitrate bt_j, parameter $s_{i,k}$, initial condition x_0 and y_0, repetition times ϱ, and replication times $\bar{j}$, value n.
Output: The encrypted content.
Initialize: The original content size is transformed by formula (4)
while $\varrho > 0$ **do**
  The content is partitioned by formulas (5) and (6).
  for $\hat{n} = 1 : S_{i,k}$ **do**
    A chaos sequence is generated by formula (8).
    The new chaos sequence is selected with value n.
    The order of bytes in row $\hat{n}$th is transformed by the new chaos sequence.
    Do the reversible operation for each byte.
    The new initial value of chaos sequence is calculated by formulas (10) and (11).
  end for
  for $\hat{m} = 1 : M_{i,k}$ **do**
    The chaos sequence is generated by formula (8).
    The new chaos sequence is selected with value n.
    The order of bytes in column $\hat{m}$th is transformed by the new chaos sequence.
    Do the reversible operation for each byte.
    The new initial value of chaos sequence is calculated by formulas (10) and (11).
  end for
  $\varrho = \varrho - 1$.
end while
The encrypted content is replicated to $\tilde{j}$ copies.

B. Auction-Game-Based Optimal Cloud Servers Selection

After the encryption on the cached content, the encrypted content needs be stored in the remote cloud servers. Here, the cloud servers are selected by edge nodes to store contents based on the optimal performance including the optimal price and the optimal strategy of each edge node. We use the auction game to select the optimal cloud servers. After sending content information to cloud servers, each cloud server then offers a bid to win the auction game and maximize its utility. The utility function of the cloud server j can be defined as

$$u_j = \alpha_j(p_j - c_j) \quad (12)$$

where α_j is a binary variable and p_j is the bid price of cloud server j. Here, we have $\alpha_j = 1$, if cloud server j wins the game. Otherwise, $\alpha_j = 0$. c_j is the cost function of cloud server j. As the cloud servers in the auction are rational, the bid of cloud server j should be no lower than its cost for storing the content. We have

$$c_j \leq p_j. \quad (13)$$

Indeed, the cost of a cloud server is usually private and cannot be known by other cloud servers. But each cloud server can estimate the others' cost by the uniform distribution as follows:

$$f(c) = \begin{cases} \frac{1}{C_{\max} - C_{\min}}, & \text{if } C_{\min} < c < C_{\max} \\ 0, & \text{otherwise} \end{cases} \quad (14)$$

After receiving bids from all candidates of cloud servers, the edge node i will select the optimal cloud server, with which the utility of edge node i is the largest. The utility of edge node i

with the bid of cloud server j for mobile user k's content is

$$u_i = \frac{V_{i,j}}{p_j} \tag{15}$$

where $V_{i,j}$ is the satisfaction function of edge node i with the bid of cloud server j. Formally, $V_{i,j}$ can be defined as

$$V_{i,j} = \lambda_i \log\left(1 + \tilde{N}_k f(m_k)\left(w_1 \frac{\varepsilon_i}{\theta_j} + w_2 \frac{1}{\hat{t}_{j,k}}\right)\right). \tag{16}$$

Here, λ_i is the satisfaction parameter of edge node i. The RTO of cloud server j is denoted as θ_j. ε_i is the adjustment parameter. $\tilde{N}_k$ is the number of mobile user k's friends and $\hat{t}_{j,k}$ is the delay to deliver the content from cloud server j for mobile user k. Since the performance of the cloud server is fixed, if the cloud server increases the bid, the utility of edge node will be decreased and the edge node can select another cloud server to be a winner when the utility is not the maximum. Each cloud server has a certain probability to win the game. Let P_j denote the probability that cloud sever j wins the game. Then, the expected utility of cloud server j can be obtained by

$$E\{u_j\} = 0 \cdot (1 - P_j) + (p_j - c_j) \cdot P_j. \tag{17}$$

Each cloud server has a target to maximize its utility. Based on these targets, the determination of the bid is the price of server. Thus, the optimization problem for cloud server j can be obtained by

$$\begin{aligned} &\max_{p_j} \ E\{u_j\} \\ &\text{s.t.} \quad p_j \geq c_j. \end{aligned} \tag{18}$$

It is noted that the target of edge node i is to select some cloud servers, with the bid of which the edge node i can obtain the maximum utility. Then, we have

$$u^*_{i,j} = \max\{u_{i,j} | j = 1, 2, \ldots, J\}. \tag{19}$$

Based on the above, each cloud server can determine its optimal bid, as shown in Theorem 1.

Theorem 1: The optimal price of backup service determined by the cloud server j is

$$\begin{aligned} {p_j}^* = &\frac{(J-1)\overline{\delta}_{i,j} c_j + C_{\max}}{J\overline{\delta}_{i,j}} \\ &- \frac{(C_{\max})^J}{J\overline{\delta}_{i,j}} \left(C_{\max} - \overline{\delta}_{i,j} c_j\right)^{-(J-1)}. \end{aligned} \tag{20}$$

Proof: For cloud server j, the bid strategy to win the auction by competing with other cloud servers is given by $p_j = \varphi(c_j)$, where $\varphi(\cdot)$ is the strategy function with respect to the cost. Since each cloud server is rational, p_j increases with c_j. According to formula (19), cloud server j can obtain the payoff only when its bid can provide the largest utility for the edge node. Otherwise, the payoff of the cloud server is zero. Thus, the probability P_j also means that the bid of the cloud server j offers the highest utility for the edge node among all candidate cloud servers. It can be obtained by

$$\begin{aligned} P_j &= \prod_{j'=1, j' \neq j}^{J} \Pr\{u_{i,j} \geq u_{i,j'}\} \\ &= \prod_{j'=1, j' \neq j}^{J} \Pr\left\{\frac{V_{i,j}}{p_j} \geq \frac{V_{i,j'}}{p_{j'}}\right\} \\ &= \prod_{j'=1, j' \neq j}^{J} \Pr\left\{p_{j'} \geq \frac{p_j V_{i,j'}}{V_{i,j}}\right\}. \end{aligned} \tag{21}$$

As mentioned above, the bid of a cloud server is based on the cost. Thus, we have

$$\begin{aligned} \Pr\left\{p_{j'} \geq \frac{p_j V_{i,j'}}{V_{i,j}}\right\} &= \Pr\left\{\varphi^{-1}(p_{j'}) \geq \frac{\varphi^{-1}(p_j) V_{i,j'}}{V_{i,j}}\right\} \\ &= \Pr\left\{c_{j'} \geq \frac{\varphi^{-1}(p_j) V_{i,j'}}{V_{i,j}}\right\}. \end{aligned} \tag{22}$$

Since a cloud server cannot have the entire information about the bids of other cloud servers, the probability of formula (22) cannot be obtained by the bids. As the cost of cloud server follows the uniform distribution, we have

$$\begin{aligned} \Pr\left\{p_{j'} \geq \frac{p_j V_{i,j'}}{V_{i,j}}\right\} &= \Pr\left\{c_{j'} \geq \frac{\varphi^{-1}(p_j) V_{i,j'}}{V_{i,j}}\right\} \\ &= \int_{\frac{\varphi^{-1}(p_j) V_{i,j'}}{V_{i,j}}}^{C_{\max}} f(c) dc. \end{aligned} \tag{23}$$

Therefore, the probability P_j can be calculated by

$$\begin{aligned} P_j &= \prod_{j'=1, j' \neq j}^{J} \Pr\left\{p_{j'} \geq \frac{p_j V_{i,j'}}{V_{i,j}}\right\} \\ &= \prod_{j'=1, j' \neq j}^{J} \int_{\delta_{i,j,j'} \varphi^{-1}(p_j)}^{C_{\max}} f(c) dc. \end{aligned} \tag{24}$$

Here, $\delta_{i,j,j'} = \frac{V_{i,j'}}{V_{i,j}}$. Let $H(p_j) = \log(P_j)$ and we have

$$\begin{aligned} H(p_j) &= \log\left(\prod_{j'=1, j' \neq j}^{J} \int_{\delta_{i,j,j'} \varphi^{-1}(p_j)}^{C_{\max}} f(c) dc\right) \\ &= \sum_{j'=1, j' \neq j}^{J} \log\left(\int_{\delta_{i,j,j'} \varphi^{-1}(p_j)}^{C_{\max}} f(c) dc\right). \end{aligned} \tag{25}$$

Then, the expected utility of cloud server j can be rewritten as

$$E\{u_j\} = (p_j - c_j) \exp(H(p_j)). \tag{26}$$

By taking the first derivation of $E\{u_j\}$ with respect to p_j, we have

$$\frac{\partial E\{u_j\}}{\partial p_j} = \exp(H(p_j)) + (p_j - c_j) \exp(H(p_j)) \dot{H}(p_j) \tag{27}$$

where $\dot{H}(p_j)$ is the first derivation of $H(p_j)$ with respect to p_j. It can be denoted by

$$\dot{H}(p_j) = \sum_{j'=1,j'\neq j}^{J} \frac{-\delta_{i,j,j'} f(\delta_{i,j,j'}\varphi^{-1}(p_j))}{\varphi'(\varphi^{-1}(p_j)) \int_{\delta_{i,j,j'}\varphi^{-1}(p_j)}^{C_{\max}} f(c)dc}. \quad (28)$$

Let $\frac{\partial E\{u_j\}}{\partial p_j} = 0$, it becomes

$$1 - (p_j - c_j) \sum_{j'=1,j'\neq j}^{J-1} \frac{\delta_{i,j,j'} f(\delta_{i,j,j'}\varphi^{-1}(p_j))}{\varphi'(\varphi^{-1}(p_j)) \int_{\delta_{i,j,j'}\varphi^{-1}(p_j)}^{C_{\max}} f(c)dc} = 0. \quad (29)$$

If p_j is the optimal biding price of cloud server j, we have $\varphi^{-1}(p_j) = c_j$ and formula (29) becomes

$$1 - (\varphi(c_j) - c_j) \sum_{j'=1,j'\neq j}^{J-1} \frac{\delta_{i,j,j'} f(\delta_{i,j,j'}c_j)}{\varphi'(c_j) \int_{\delta_{i,j,j'}c_j}^{C_{\max}} f(c)dc} = 0. \quad (30)$$

Let $\Omega(\delta_{i,j,j'}c_j) = \int_{\delta_{i,j,j'}c_j}^{C_{\max}} f(c)dc$, we have

$$1 - (\varphi(c_j) - c_j) \sum_{j'=1,j'\neq j}^{J} \frac{\delta_{i,j,j'} f(\delta_{i,j,j'}c_j)}{\varphi'(c_j)\Omega(\delta_{i,j,j'}c_j)} = 0. \quad (31)$$

Then, formula (31) can be rewritten by

$$\varphi'(c_j) - \varphi(c_j)\mathcal{F}_{i,j} = -c_j\mathcal{F}_{i,j} \quad (32)$$

where

$$\mathcal{F}_{i,j} = \sum_{j'=1,j'\neq j}^{J} \frac{\delta_{i,j,j'} f(\delta_{i,j,j'}c_j)}{\Omega(\delta_{i,j,j'}c_j)}. \quad (33)$$

By solving formula (33), the optimal bidding of cloud server becomes

$$\varphi(c_j) = e^{\int \mathcal{F}_{i,j}dc_j} \int_0^{c_j} -\omega\mathcal{F}_{i,j} e^{-\int \mathcal{F}_{i,j}d\omega} d\omega. \quad (34)$$

where ω is the integrable variable. Here, the price becomes zero when the cost is zero. Since the cost of cloud server follows the uniform distribution with $[C_{\min}, C_{\max}]$, we have

$$\mathcal{F}_{i,j} = \sum_{j'=1,j'\neq j}^{J-1} \frac{\delta_{i,j,j'} \frac{1}{C_{\max}-C_{\min}}}{\frac{C_{\max}-\delta_{i,j,j'}c_j}{C_{\max}-C_{\min}}} = \sum_{j'=1,j'\neq j}^{J-1} \frac{\delta_{i,j,j'}}{C_{\max} - \delta_{i,j,j'}c_j}. \quad (35)$$

It becomes as follows:

$$e^{\int F_{i,j}dc_j} = e^{\int \sum_{j'=1,j'\neq j}^{J-1} \frac{\delta_{i,j,j'}}{C_{\max}-\delta_{i,j,j'}c_j} dc_j} = \prod_{j'=1,j'\neq j}^{J-1} (C_{\max} - \delta_{i,j,j'}c_j)^{-1}. \quad (36)$$

And, we have

$$\begin{aligned}
&\int_0^{c_j} -\omega\mathcal{F}_{i,j} e^{-\int \mathcal{F}_{i,j}d\omega} d\omega \\
&= \int_0^{c_j} -\omega \left(\sum_{j'=1,j'\neq j}^{J} \frac{\delta_{i,j,j'}}{C_{\max} - \delta_{i,j,j'}y} \right) \\
&\times \prod_{j'=1,j'\neq j}^{J} (C_{\max} - \delta_{i,j,j'}\omega)d\omega \\
&= \int_0^{c_j} -\omega \sum_{j'=1,j'\neq j}^{J} \left(\delta_{i,j,j'} \left(\prod_{j''=1,j''\neq j,j'}^{J} (C_{\max} - \delta_{i,j,j''}\omega) \right) \right) d\omega \\
&= \sum_{j'=1,j'\neq j}^{J} \int_0^{c_j} -\omega\delta_{i,j,j'} \left(\prod_{j''=1,j''\neq j,j'}^{J} (C_{\max} - \delta_{i,j,j''}\omega) \right) d\omega \\
&\approx c_j(C_{\max} - \overline{\delta}_{i,j}c_j)^{J-1} + \frac{(C_{\max} - \overline{\delta}_{i,j}c_j)^J}{J\overline{\delta}_{i,j}} - \frac{(C_{\max})^J}{J\overline{\delta}_{i,j}}
\end{aligned} \quad (37)$$

where $\overline{\delta}_{i,j}$ can be calculated by

$$\overline{\delta}_{i,j} = \frac{\sum_{j'=1,j'\neq j}^{J} \delta_{i,j}}{J-1}. \quad (38)$$

By substituting (36) and (37) into (34), the optimal bidding price of cloud server j becomes

$$\begin{aligned}
p_j{}^* = \varphi(c_j) = &\frac{(J-1)\overline{\delta}_{i,j}c_j + C_{\max}}{J\overline{\delta}_{i,j}} \\
&- \frac{(C_{\max})^J}{J\overline{\delta}_{i,j}} (C_{\max} - \overline{\delta}_{i,j}c_j)^{-(J-1)}.
\end{aligned} \quad (39)$$

Thus, Theorem 1 is proved. ■

From formula (39), we can see that the optimal bidding strategy of cloud server j is a function of its cost. Therefore, we analyze the cost of cloud server j for edge node i. According to the status of cloud server, the cost of cloud server j for storing the content can be defined as follows:

1) RTO

The cost becomes high when the RTO is low. In other words, the bid of cloud server j increases when its RTO is reduced. Thus, we have

$$c_j^1 = \zeta_j^1 \log\left(1 + \frac{\max(\theta_j)}{\theta_j}\right) \quad (40)$$

where ζ_j^1 is the parameter of cloud server to describe the cost of RTO.

2) The size of content

Since it tasks the cost to store contents in cloud server, cloud server j will require a high price to the edge node if the size of content is large. In comparison, when the size of content is small, a low price will declare. We have

$$c_j^2 = \zeta_j^2 D_{i,k} \quad (41)$$

where ζ_j^2 is the parameter of cloud server to describe the cost of unit size of content. In addition, the popularity and the number

TABLE I
SIMULATION PARAMETERS

Parameters	Values
b, the bandwidth between two route nodes	100Mbps
λ_i, the satisfaction parameter of edge node i	1
ε_i, the adjustment parameter of edge node i	1
ζ_j^1, the parameter of cloud server j for the cost of RTO with unit time	[0.6, 0.8]
ζ_j^2, the parameter of cloud server j for the cost of unit content size	[0.1, 0.3]
ξ_j, the adjustment parameter for cost of edge node j	0.1

of social friends also have effects on the cost. The cost can be defined as

$$c_j = \xi_j f(m_k)\tilde{N}_k \left(\zeta_j^1 \log\left(1+\frac{\max(\theta_j)}{\theta_j}\right)+\zeta_j^2 D_{i,k}\right) \quad (42)$$

where ξ_j is the adjustment parameter of cloud server j.

After the cloud servers decide their optimal bids, i.e., $\{p_1{}^*, p_2{}^*, \ldots, p_j{}^*, \ldots, p_J{}^*\}$, the edge node i selects $\tilde{j}$ cloud servers which offer the best utilities.

V. PERFORMANCE EVALUATION

In this section, we conduct the extensive simulation to evaluate the performance of the proposed scheme. The simulation setup is first introduced, followed by the numerical results and analysis.

A. Simulation Setup

In the simulation with the simulator coded by Matlab, the number of mobile users is 100, and the number of edge nodes is 20. Besides, the number of cloud servers is 10. The probability that a cloud server is attacked by adversaries and lose the content is uniformly distributed in $[0.6, 0.8]$. Initially, the social relation degrees among mobile users are randomly set within $[0, 1]$. If the social relation degree of two mobile users is larger than a threshold, these mobile users are seen as friends. The parameter of content popularity is 0.5. In addition, the RTO is uniformly distributed in $[1, 5]$. The set of bite rate generated by content is selected at random from [0.2, 0.4, 1.7, 1.3, 2.3] Mbps. The minimum length of a content is 2 s and the maximum length is 10 s. The number of route nodes is randomly in $[10, 50]$. Other parameters are concluded in Table I.

The following metrics are used to evaluate the performance:

1) *Security to price ratio (SPR):* The ratio of security probability to the price of storing content. The SPR can be defined as follows:

$$\mathrm{SPR}(\tilde{j}) = \frac{\mathrm{SP}}{p_{i,1}^* + \upsilon \cdot \left(\sum_{j=1}^{\tilde{j}} p_{i,j}^* - p_{i,1}^*\right)}. \quad (43)$$

Here, SP is the security probability of the stored content which is replicated and stored in $\tilde{j}$ cloud servers. υ is the increasing step for edge node i.

2) *Average utility of an edge node:* The average utility of an edge node to store contents in multiple cloud servers, defined by

$$AU(\tilde{j}) = \frac{\sum_{j=1}^{\tilde{j}} u_{i,j}}{\tilde{j}} \quad (44)$$

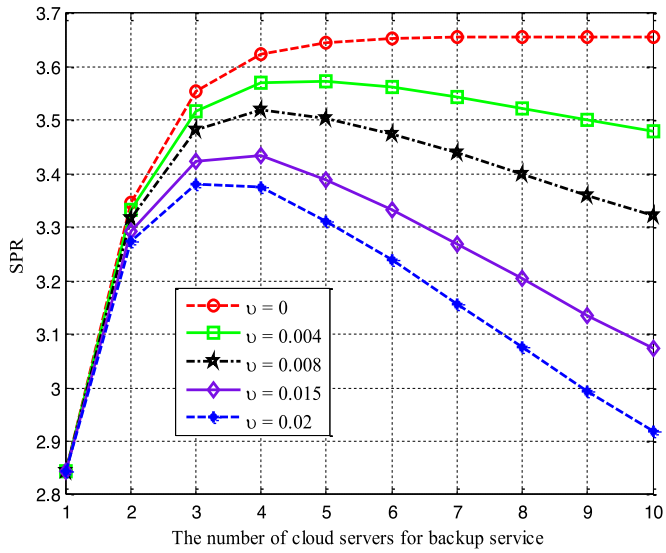


Fig. 2. Ratio of security to price of an edge node vs. the number of selected cloud servers.

B. Numerical Results

The proposed scheme is compared with two conventional schemes as below:

Random scheme (RS) : In this scheme, each edge node randomly selects a cloud servers to store content. And the cloud randomly determines the price of service.

The scheme without price [43]*:* In this scheme, each edge node selects the optimal cloud servers based on the provided service without the consideration of the required prices.

Fig. 2 shows the SPR of an edge node when the number of selected optimal cloud servers changes in the proposed scheme. In this simulation, there are five increasing step values which are 0, 0.004, 0.008, 0.015, and 0.02, respectively. From Fig. 2, it can be seen that the SPR of the edge node increases at first and then decreases with the increase of the number of selected optimal cloud servers. The security probability increases fast when a few cloud servers are selected. And the probability reaches to be stable when more cloud servers are selected as the optimal. In addition, when υ is large, the SPR of an edge node decreases early and fast. Here, the larger υ means that the edge node pays more attention to the cost, inducing the SPR is sensitive to the prices of cloud servers.

Fig. 3 is the SPR of an edge node in the proposed scheme by the comparison with other conventional schemes, where the number of selected cloud servers is changed from 1 to 10. Here, the increasing step υ is 0.01. From Fig. 3, it can be observed that the proposed scheme has the largest value of SPR. In the proposed scheme, the optimal cloud servers are selected based on the utility of the edge node, where both the performance of

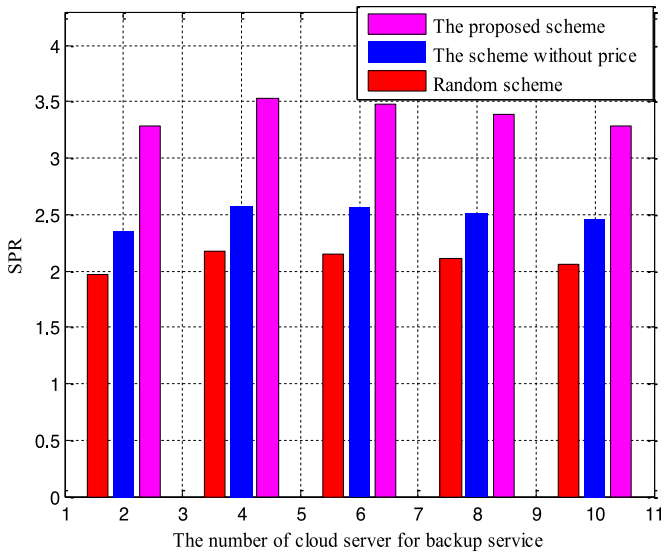


Fig. 3. Schemes comparison on the ratio of security to price of an edge node.

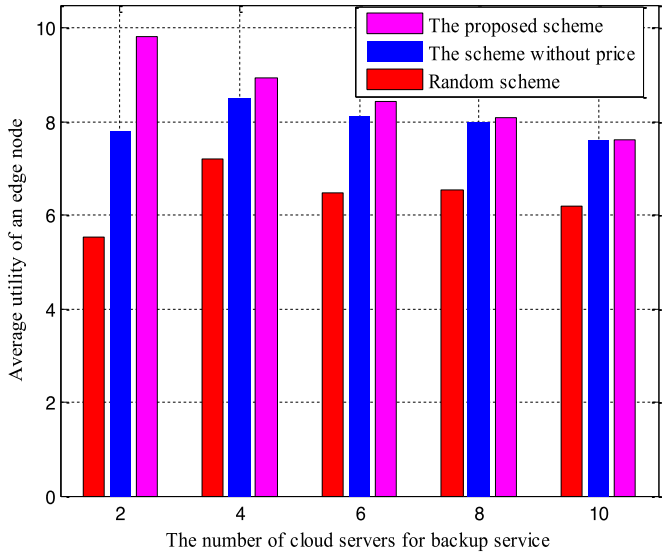


Fig. 5. Schemes comparison on the average utility of an edge node.

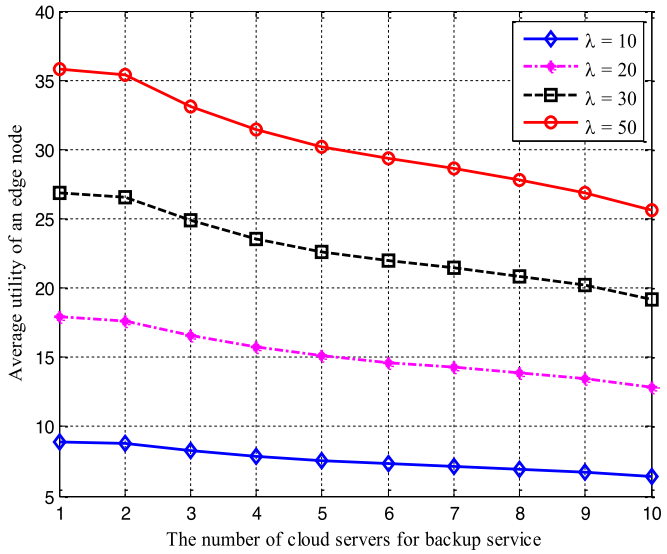


Fig. 4. Average utility of an edge node vs. the number of selected cloud servers.

each cloud server and the price are considered. In the random scheme, the cloud server is randomly selected where the price may be high. In the scheme without price, the cloud servers are selected based on the performance with the result that these cloud services usually have high prices.

Fig. 4 shows the average utility of an edge node when the number of the selected optimal cloud servers in the proposal is changed from 1 to 10. Four satisfaction parameters which are 10, 20, 30, and 50 are used to show the result, respectively. From Fig. 4, we can see that the average utility gradually decreases with the increasing number of the selected cloud servers. The reason is that the selected cloud servers is sorted by the power on the utility of edge node. Namely, the optimal cloud server can offer the maximum utility for edge node. Thus, the average utility decreases when more cloud servers are selected.

Fig. 5 shows the average utility of an edge node in the proposed scheme by the comparison with other convention schemes. In the simulation, the number of the selected optimal cloud servers is changed from 1 to 10. The satisfaction parameter is 10 and other settings are unchanged. From Fig. 5, it can be observed that the proposed scheme outperforms other schemes with the largest value of average utility. The optimal cloud servers are selected based on the offered utilities for the edge node in the proposed scheme. However, in the random scheme, the selected cloud server is randomly selected where the large utility cannot be offered for the edge node. In the scheme without price, the selected cloud servers may have high price while offering low utilities for the edge node.

VI. Conclusion

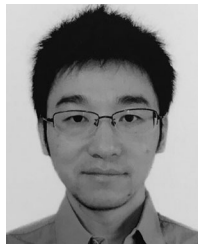
This paper has presented a secure content caching scheme for disaster backup in MSNs. First, in order to keep the privacy of content, the scrambling and partitioning method has been introduced to encrypt the content. After that, to realize the integrality of content, the encrypted content is delivered and stored in multiple cloud servers. Then, an auction game model is developed to select the optimal cloud servers where both the edge node and the selected servers can achieve maximum utilities. At last, the simulation results show that the proposed scheme outperforms other conventional schemes by improving security and resource efficiency. The future work is to optimally distribute the secure storage for content in cloud servers to save resource and reduce cost.

References

[1] D. Wang, H. Cheng, D. He, and P. Wang, "On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices," *IEEE Syst. J.*, vol. 12, no. 1, pp. 916–925, Mar. 2018.

[2] Q. Xu, Z. Su, and S. Guo, "A game theoretical incentive scheme for relay selection services in mobile social networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6692–6702, Aug. 2016.

[3] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html
[4] 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, DOI: 10.1109/TVT.2018.2824345.
[5] D. Zhang *et al.*, "Energy-harvesting-aided spectrum sensing and data transmission in heterogeneous cognitive radio sensor network," *IEEE Trans. Veh. Technol.*, vol. 66, no. 1, pp. 831–843, Jan. 2017.
[6] X. Liu, Y. Liu, N. Xiong, N. Zhang, A. Liu, H. Shen, and C. Huang, "Construction of large-scale low-cost deliver infrastructure using vehicular networks," *IEEE Access*, vol. 6, pp. 21482–21497, Apr. 2018
[7] Y. Liu, A. Liu, S. Guo, Z. Li, Y. J. Choi, and H. S, "Context-aware collect data with energy efficient in cyber-physical cloud systems," *Future Generation Comput. Syst.*, to be published.
[8] Y. Xiao, X. Du, J. Zhang, F. Hu, and S. Guizani, "Internet protocol television (IPTV): The killer application for the next-generation internet", *IEEE Commun. Mag.*, vol. 45, no. 11, pp. 126–134, Nov. 2007.
[9] Z. Su and Q. Xu, "Security-aware resource allocation for mobile social big data: A matching-coalitional game solution," *IEEE Trans. Big Data*, pp. 1–1, May 2017. DOI: 10.1109/TBDATA.2017.2700318.
[10] Y. Xiao, V. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," *J. Comput. Commun.*, vol. 30, no. 11–12, pp. 2314–2341, 2007.
[11] Y. Cheng, X. Fu, X. Du, B. Luo, and M. Guizani, "A lightweight live memory forensic approach based on hardware virtualization," *Elsevier Inf. Sci.*, vol. 379, pp. 23–41, 2017.
[12] 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. Inform.*, vol. 14, no. 6, pp. 2550–2559, Jun. 2018, DOI: 10.1109/TII.2017.2787201.
[13] Q. Xu, Z. Su, and K. Yang, "Optimal control theory-based epidemic information spreading scheme for mobile social users with energy constraint," *IEEE Access*, vol. 5, pp. 14107–14118, 2017.
[14] L. Wu, X. Du, and J. Wu, "Effective defense schemes for phishing attacks on mobile computing platforms," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6678–6691, Aug. 2016.
[15] J. Zhou, R. Hu, and Y. Qian, "Scalable distributed communication architectures to support advanced metering infrastructure in smart grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1632–1642, Sep. 2012.
[16] Z. Su, Y. Hui, T. Luan, and S. Guo, "Engineering a game theoretic access for urban vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 4602–4615, Jun. 2017.
[17] F. Ma, X. Liu, A. Liu, M. Zhao, H. Changqin, and T. Wang, "A time and location correlation incentive scheme for deeply data gathering in crowdsourcing networks," *Wireless Commun. Mobile Comput.*, vol. 2018, 2018, Art.ID. 8052620.
[18] M. Wu, Y. Wu, X. Liu, M. Ma, A. Liu, and M. Zhao, "Learning based synchronous approach from forwarding nodes to reduce the delay for industrial internet of things," *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 10, pp. 1–22, 2018.
[19] N. Lu, N. Cheng, N. Zhang, X. Shen, J. Mark, and F. Bai, "Wi-fi hotspot at signalized intersection: Cost-effectiveness for vehicular internet access," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, pp. 3506–3518, May 2016.
[20] Q. Xu, Z. Su, B. Han, D. Fang, Z. Xu, and X. Gan,"Analytical model with a novel selfishness division of mobile nodes to participate cooperation," *Peer-to-Peer Netw. Appl.*, vol. 9, no. 4, pp. 712–720, 2016.
[21] C. Wu, T. Yoshinaga, Y. Ji, T. Murase, and Y. Zhang, "A reinforcement learning-based data storage scheme for vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 6336–6348, Jul. 2017.
[22] M. Huang, A. Liu, T. Wang, and C. Huang, "Green data gathering under delay differentiated services constraint for internet of things," *Wireless Commun. Mobile Comput.*, vol. 2018, 2018, Art.ID. 9715428, DOI: 10.1155/2018/9715428.
[23] D. Wu, J. Wang, R. Hu, Y. Cai, and L. Zhou, "Energy-efficient resource sharing for mobile device-to-device multimedia communications", *IEEE Trans. Veh. Technol.*, vol. 63, no. 5, pp. 2093–2103, Jun. 2014.
[24] X. Hu, T. Chu, V. Leung, E. Ngai, P. Kruchten, and H. Chan, "A survey on mobile social networks: Applications, platforms, system architectures, and future research directions," *IEEE Commun. Surveys Tut.*, vol. 17, no. 3, pp. 1557–1581, Thirdquarter 2015.
[25] Z. Su, Q. Xu, F. Hou, Q. Yang, and Q. Qi, "Edge caching for layered contents in mobile social networks," *IEEE Trans. Multimedia*, vol. 19, no. 10, pp. 2210–2221, Oct. 2017.
[26] J. Li, H. Yan, Z. Liu, X. Chen, X. Huang, and D. Wong, "Location-sharing systems with enhanced privacy in mobile online social networks," *IEEE Syst. J.*, vol. 11, no. 2, pp. 439–448, Jun. 2017.
[27] F. Abbas, U. Rajput, and H. Oh, "PRISM: PRivacy-aware interest sharing and matching in mobile social networks," *IEEE Access*, vol. 4, pp. 2594–2603, May 2016.
[28] C. Xu, C. Gao, Z. Zhou, Z. Chang, and Y. Jia, "Social network-based content delivery in device-to-device underlay cellular networks using matching theory," *IEEE Access*, vol. 5, pp. 924–937, Nov. 2016.
[29] T. Ning, Y. Liu, Z. Yang, and H. Wu, "Incentive mechanisms for data dissemination in autonomous mobile social networks," *IEEE Trans. Mobile Comput.*, vol. 16, no. 11, pp. 3084–3099, Nov. 2017.
[30] C. Liang, Y. He, F. Yu, and N. Zhao, "Enhancing QoE-aware wireless edge caching with software-defined wireless networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 10, pp. 6912–6925, Oct. 2017.
[31] X. Xu, J. Liu, and X. Tao, "Mobile edge computing enhanced adaptive bitrate video delivery with joint cache and radio resource allocation," *IEEE Access*, vol. 5, pp. 16406–16415, Aug. 2017.
[32] B. Zhou, Y. Cui, and M. Tao, "Optimal dynamic multicast scheduling for cache-enabled content-centric wireless networks," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 2956–2970, Jul. 2017.
[33] X. Li, X. Wang, K. Li, Z. Han, and V. C. M. Leung, "Collaborative multi-tier caching in heterogeneous networks: Modeling, analysis, and design," *IEEE Trans. Wireless Commun.*, vol. 16, no. 10, pp. 6926–6939, Oct. 2017.
[34] J. Song, M. Sheng, T. Quek, C. Xu, and X. Wang, "Learning-based content caching and sharing for wireless networks," *IEEE Trans. Commun.*, vol. 65, no. 10, pp. 4309–4324, Oct. 2017.
[35] D. Malak, M. Al-Shalsh, and J. Andrews, "Spatially correlated content caching for device-to-device communications," *IEEE Trans. Wireless Commun.*, vol. 17, no. 1, pp. 56–70, Jan. 2018.
[36] F. Chen, T. Xiang, Y. Yang, and S. Chow, "Secure cloud storage meets with secure network coding," *IEEE Trans. Comput.*, vol. 65, no. 6, pp. 1936–1948, Jun. 2016.
[37] H. Tian *et al.*, "Dynamic-hash-table based public auditing for secure cloud storage," *IEEE Trans. Serv. Comput.*, vol. 10, no. 5, pp. 701–714, Sep. 2017.
[38] Y. Tang, P. Lee, J. Lui, and R. Perlman, "Secure overlay cloud storage with access control and assured deletion," *IEEE Trans. Depend. Sec. Comput.*, vol. 9, no. 6, pp. 903–916, Nov. 2012.
[39] J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 8, pp. 1931–1940, Aug. 2017.
[40] H. Lin and W. Tzeng, "A secure erasure code-based cloud storage system with secure data forwarding," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 6, pp. 995–1003, Jun. 2012.
[41] X. Li, H. Wang, S. Yi, and X. Yao, "Receiving-capacity-constrained rapid and fair disaster backup for multiple data centers in SDN," in *Proc. IEEE Int. Conf. Commun.*, Paris, France, 2017, pp. 1–6.
[42] X. Xie, Q. Ling, P. Lu, W. Xu, and Z. Zhu, "Evacuate before too late: Distributed backup in inter-dc networks with progressive disasters," *IEEE Trans. Parallel Distrib. Syst.*, vol. 29, no. 5, pp. 1058–1074, May 2018.
[43] Z. Su, Q. Qi, Q. Xu, and S. Guo, "Incentive scheme for cyber phyical social systems based on user behaviors," *IEEE Trans. Emerg. Topics Comput.*, pp. 1–1, Feb. 2017. DOI: 10.1109/TETC.2017.2671843.
[44] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," *Pattern Recog. Lett.*, vol. 31, no. 5, pp. 347–354, 2010.



Zhou Su received the Ph.D. degree from Waseda University, Tokyo, Japan, in 2003.

He is currently an Associate Editor with the IET Communications and IEICE Transactions on Communications. He is the Chair of the Multimedia Services and Applications over Emerging Networks Interest Group of the IEEE Comsoc Society and the Multimedia Communications Technical Committee. He also served as the Cochair of several international conferences including IEEE VTC Spring 2016, IEEE CCNC 2011, etc. He is a TPC Member of some flagship conferences including IEEE INFOCOM, IEEE ICC, IEEE Globecom, etc. His research interests include multimedia communication, wireless communication, and network traffic.

Dr. Su was the recipient of IEEE CyberSciTech2017, WiCon2016, CHINACOM2008, and Funai Information Technology Award for Young Researchers, in 2009.

Qichao Xu is currently working toward the Ph.D. degree with the School of Mechatronic Engineering and Automation, Shanghai University, Shanghai, China. His research interests include the general area of wireless network architecture and vehicular networks.

Jun Luo received the Bachelor and Master degrees in mechanical engineering from Henan Polytechnic University, Henan, China, and the Ph.D. degree in mechanical engineering from Shanghai Jiao Tong University, Shanghai, China, in 1994, 1997, and 2000, respectively.

He is currently a Professor with Shanghai University, Shanghai, China, Discipline Leader of mechanical engineering with Shanghai Plateau Disciplines, holder of National Science Fund for Distinguished Young Scholars, one of the Leading Talents of Shanghai, Shanghai Subject Chief Scientist, Shuguang Scholar, holder of Shanghai Rising-Star Program (followup), Vice Dean with School of Mechatronic Engineering and Automation, Member of 14th Expert Review Committee of Department of Information Sciences of National Natural Science Foundation of China.

Dr. Luo mainly works on the structure, sensing and control technique of advanced robots, and undertakes more than 30 projects, including miniature unmanned vehicle, underwater robots, south-polar robot, nuclear power station robots, biomimetic eye movement control, and USVs. He is the recipient of many honors, including Second level prize of National Technology Invention Award, first level prize of Shanghai Technology Invention Award, first level prize of Shanghai Science and Technology Progress Award, first level Science and Technology Prize of China Institute of Navigation, Tutor Award of Hiwin Doctoral Dissertation Award, IEEE Best Paper in Biomimetics, IEEE ICRA Best Student Paper Award, and IEEE ICRA Best Manipulation Paper Award Finalist.

Huayan Pu received the M.Sc. and Ph.D. degrees in mechatronics engineering from Huazhong University of Science and Technology, Wuhan, China, in 2007 and 2011, respectively.

She is currently a Professor with the School of Mechatronics Engineering and Automation, Shanghai University, Shanghai, China. Her research interests include modeling, control, and simulation of field robotics and locomotion system.

Dr. Pu was the recipient of the best paper in biomimetics at the 2013 IEEE International Conference on Robotics and Biomimetics. She was also nominated as the best conference paper finalist at the 2012 IEEE International Conference on Robotics and Biomimetics.

Yan Peng received the Ph.D. degree in pattern recognition and intelligent systems from Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang, China, in 2009.

She is currently a Professor with Shanghai University, Shanghai, China, and also involved with the Executive Dean of Research Institute of USV Engineering, Shanghai, China. Her research interests include modeling and control of unmanned surface vehicles, field robotics, and locomotion system.

Rongxing Lu has been an Assistant Professor with the Faculty of Computer Science, University of New Brunswick, Fredericton, NB, Canada, since August 2016. Before that, he was an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from April 2013 to August 2016. He worked as a Postdoctoral Fellow with the University of Waterloo, Waterloo, ON, Canada, from May 2012 to April 2013. His research interests include applied cryptography, privacy enhancing technologies, and IoT-Big Data security and privacy.

Dr. Lu was the recipient of the most prestigious Governor Generals Gold Medal, when he received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, in 2012, and the 8th IEEE Communications Society (ComSoc) Asia Pacific Outstanding Young Researcher Award, in 2013. He is currently a Senior Member of IEEE Communications Society. He has published extensively in his areas of expertise, and was the recipient of nine best (student) paper awards from reputable journals and conferences. Currently, he serves as the Vice-Chair (Publications) of IEEE ComSoc CIS-TC (Communications and Information Security Technical Committee). He is the recipient of 2016–2017 Excellence in Teaching Award, FCS, UNB.