International Research Journal of Computer Science (IRJCS) ISSN: 2393-9842
Issue 06, Volume 6 (June 2019) www.irjcs.com
SPECIAL ISSUE - 5th International Conference - "ACCE – 2019"

SECURITY-AWARE RESOURCE ALLOCATION FOR MOBILE SOCIAL BIG DATA

Mrs. Shilpa G V[1], Arshatha Parthasarathy[2], Keerthana M R[3]
[1]Asst. Professor Dept. of CSE, Vemana Institute of Technology, Bangalore.
[2]Student Dept. of CSE, Vemana Institute of Technology, Bangalore.
[3]Student Dept. of CSE, Vemana Institute of Technology, Bangalore.
[1]shilpa.gvs@gmail.com, [2]arshathajaidhev@gmail.com, [3]keerthi0705@gmail.com

Manuscript History
Number: IRJCS/RS/Vol.06/Issue06/JNCS10110
Received: 29, May 2019
Final Correction: 30, May 2019
Final Accepted: 02, June 2019
Published: June 2019
doi://10.26562/IRJCS.2019.JNCS10110
Editor: Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India

ABSTRACT -As both the scale of mobile networks and the population of mobile users keep increasing, the applications of mobile social big data have emerged where mobile social users can use their mobile devices to exchange and share contents with each other. The security resource is needed to protect mobile social big data during the delivery. However, due to the limited security resource, how to allocate the security resource becomes a new challenge. Therefore, in this paper a model for a joint matching-coalitional game based security-aware resource allocation scheme to deliver mobile social big data, is presented. In this scheme, firstly a coalition game model is introduced for base stations (BSs) to form groups to provide both wireless and security resource, where the resource efficiency can be improved. Next, a joint matching-coalition algorithm is presented to obtain the stable security-aware resource allocation. At last, the simulation experiments prove that the presented scheme outperforms other existing schemes by providing higher efficiency and resource utilization for both wireless and security resources.
KEYWORDS –Mobile social network, big data, security resource, matching theory, and coalition game.

I. INTRODUCTION

Recently, with the development of the communication technologies and devices, an ever-increasing amount of mobile social big data are being delivered among mobile social users by various applications, such as multimedia streaming, healthcare services, etc. Especially, with the emerging mobile social networks (MSNs), people in different locations can form communities to exchange and share mobile data [1]- [2], which have properties of a large volume, variety, value and velocity. Related report [3] shows that the traffic of mobile data will be nearly eightfold in 2020, compared with that in 2015. It can be predicted that the applications of mobile social big data will play an important role in our future. For the applications of mobile social big data, security issues should be taken into consideration. For example, the location information is critical to mobile users as the disclose of location may reveal what mobile social users have done. In addition, the wireless connection, which is used by the users, should be protected in order to prevent the attack by the third parties. Thus, except the conventional wireless resource, the security resource such as computation resource to implement monitoring, encryption, etc., is also needed. However, as the security resource is limited, how to allocate the security resource to deliver mobile social big data becomes a new challenge. On one hand, different amount of security resource should be allocated based on different situations such as the level of threats. On the other hand, mobile social users have different social activities where different security resources are demanded to obtain social services.

Although some related studies have been carried out to study security issues in mobile networks, most of them mainly focus on how to protect the privacy of mobile social users, instead of the security resource allocation. Next, despite some works related to wireless resource, most of them are to allocate wireless resource such as bandwidth or spectrum without the consideration of security. In addition, the social features of mobile users who deliver the mobile social big data a real so needed to be discussed. Therefore, the security-aware resource to deliver mobile social big data is still an issue to be studied. In this paper, a model for security-aware resource allocation scheme to deliver mobile big data based on joint matching-coalition game, is presented. Firstly, the resource is divided two categories. The first is the wireless resource provided by base stations (BSs) for mobile social users to obtain the satisfied rates. The second is the security resource which can be seen as the computation resource in BSs to guarantee the security for the activities of users. Next, the BSs are grouped into some coalitions to provide resource together with the advantage that the resource efficiency can be improved by resource sharing. The BSs with little resource can obtain resource from other BSs which have redundant resource to lease. A joint coalition-matching algorithm is presented to obtain the stable result of security-aware resource allocation. The simulation results show that the proposed scheme provides higher efficiency and resource utilization for both wireless and security resources.

II. RELATED WORK

Recently, mobile social big data have drawn an increasing attention from both industry and academia. [4] proposed a novel incentive scheme to stimulate selfish nodes to participate in bundle delivery in MSNs.[5] provided a comprehensive survey on the MSN specifically from the perspectives of applications, network architectures, and protocol design issues. [6] investigated a mobile offloading game against smart attacks we have investigated a mobile offloading game against smart attacks, in which a security agent protects a serving AP with two defense modes. [7] proposed a game theoretic resource allocation scheme for media cloud to allocate resource to mobile social users through brokers. [8] proposed a channel-aware reputation system with adaptive detection threshold (CRS-A) to detect selective forwarding attacks in WSNs. [9] proposed a novel design for content delivery over software defined MSNs by using SDMSNs.[10] proposed a mechanism for transmit strategy adaptation using adaptive base station cooperation with security protection for physical layer security in two-cell wireless networks. [11] proposed an approach that leverages contemporary packet optimization schemes and enables ample opportunities for better performance rate by implementing packet size optimization along with effective support of multi-level security data in wireless data network. [12] designed a resource allocation model based on double-sided combinational auctions (DCA) for optimizing the performance of transparent computing.

III. OBJECTIVE AND PROBLEM STATEMENT

A. The problem statement

Below mentioned are the problems to be addressed:

i) Currently, most of the work on security issues mainly focus on how to protect the privacy of the mobile social users instead of the security resource allocation. Therefore, the first problem to be addressed is the optimal security-resource allocation.

ii) Despite the works on wireless resource allocation, the wireless resource provided by base stations for mobile social users do not obtain the satisfied rates as under the current network conditions, most communication bandwidth can't satisfy clients' requirement for QoS. Thus, the next problem to be addressed is the proposal of a scheme that improves the resource efficiency by resource sharing.

B. Objective

This paper presents a model that uses joint matching-coalitional game based security aware-resource allocation scheme to deliver mobile social big data. It aims to solve problems involving allocation of wireless and security resources where higher efficiency and resource utilization could be obtained. This in-turn affects the Quality of Experience of the users. Simulated experiments for the theoretical scheme show that the proposed method outperforms other existing met.

IV. METHODOLOGY

The methodology involves simulation of the theoretical joint matching-coaltional game-based security-aware resource allocation scheme. Before discussing the implementation of various modules present in the model in detail, the coalitional game and the security aware resource allocation algorithm for the matching-coalitional game based on which the experimental model is developed, is introduced below.

Coalitional Game for Base Stations

The amount of resource in different BSs is not the same. Some BSs may have more wireless resource with less security resource, while other BSs may have more security resource and less wireless resource. Therefore, the BSs can form the coalition to improve their utilities and resource efficiency. In a coalition, the resource can be shared by all BSs in this coalition.

Specifically, the BSs with little wireless resource can rent it from others which have more wireless resource. Similarly, the security resource also can be transmitted from the BSs with more security resource to the BSs with less security resource. In the coalition game, the BSs are modeled as the rational players where the decision of the player to join or leave a coalition is based on a utility function where coalition forming decision of any player can be made by using one of the choice: 'Join' or 'Depart' whichever leads to a higher payoff.

Module Description

The system is partitioned in tiny groups called as modules for easy coding and understand. This paper contains four modules:

- base-station allocation
- job allocation
- scheduling
- report.

These modules are briefly explained in the following sections.

A. Base-station Allocation

Every user that needs to communicate does so by means of base stations acting as an intermediary. Thus, base stations first need to be setup in order enable multiple users for communications. We consider a mobile social network with a total of I base stations (BSs). Then a number of mobile social users are created to simulate the real-world existence of mobile social users. The set of BSs created can provide wireless resource and security resource to mobile social users. There are some computation machines (e.g, virtual machines) in each BS for security implementations such as monitoring, encryption, etc. Compared with adopting security strategies in content provider in real-world, there are two advantages to place the security resource in BSs: 1) Placing security resource in BSs can detect the potential malicious users who want to attack the network by using channel information. 2) The information security can be improved by BSs for mobile social users to deliver private contents with encryption algorithms. For BS i, the total amount of security resource in it is denoted by Si, which can be seen as a form of computation resource. In addition, each BS has some wireless resource for mobile social users to deliver contents in network.

B. Job Allocation

Mobile social users may have social interactions with each other. They may also process various tasks. Each such kind of interaction can be represented as jobs. The mobile social users connect BSs to download content and acquire security resource. These users can also share the obtained wireless resource. In order to simulate such an interaction, this module allows to create jobs by users. Each job is associated with certain size(bandwidth requirements) and priorities. Such jobs with size can be allocated with the priority as a normal or deadline job. In a real-world implementation, more or less resources based on coalition, are allocated to the jobs to allow faster execution based on their priority. The detailed view of such allocation is not the focus of the experimental model. The simulation here focusses mainly on the coalition and efficiency in utilization of resources than on the job priorities. Thus, this module allows to shows the user created jobs along with their size requirements and allow these details to be sent to the further to the resource scheduler.

C. Scheduling

Mobile social users need to obtain wireless resource for wireless connection. Every job created by users needs certain resources in order to be executed. Job scheduling is a mechanism that maps jobs to appropriate resources to execute and to deliver the result efficiently based on available resource and requirement. Job scheduling is an important module in this system as this module decides to allocate resource for the user defined jobs based on the requirements. Here, the scheduler receives job status and resource status from the previous models. Then, the number of normal jobs and deadline jobs and the overloaded and underloaded base stations are calculated. These jobs are then assigned to the resources and viewed. In the real applications, the BSs are equipped with some virtual machines to provide computation resource for security. With the security computation resource, the BSs can implement encryption algorithms during the content delivery or monitor the delivering process to prevent from being attacked. In addition, each BS can also provide wireless resource to mobile users. Mobile users can obtain both security resource and wireless resource with an improved QoE. As the content delivery may be attacked by the third party, the security protocols should be adopted into BSs for protecting contents. Without losing generality, it takes some computing resource to conduct security protocols. For example, BSs need to monitor the content process to detect attacks. And encryption algorithms should be implemented during the content delivery. Both the above security measures need to consume the computing resource. Accordingly, security constraint is modeled as the computing resource constraint.

D. Report

This module simply yields the results in the form of bar charts. The reports are obtained for efficiency and resource utilization. Firstly, All the details from the resource status are obtained.

Next, total make span time is calculated, along with resource utilization. Finally, Graphical reports are obtained for Efficiency and Resource Allocation based on the calculations of performance over makespan time and the total available resources and resources utilized over memory utilization.

V. SYSTEM ARCHITECTURE

This section describes the system architecture of the simulation model developed for the experimentation of the proposed scheme. It involves a number of users performing 'n' number of processes with certain level of security resource requirement. The communication between the mobile users is done over a LAN/WAN network. Each user task (also referred to as jobs) requires transmission over a base station with certain level of requirement of wireless resource(bandwidth) as well. Each job is associated with a certain size which needs to scheduled by the job scheduler for obtaining the required resources. This is done by combining and calculating the total size of resources required by all the jobs, divide the jobs into clusters for different base stations and scheduling the jobs by assigning resources for each of the clusters by a virtual machine scheduler. This in turn allocates resources for all the jobs by creating a virtual space for the jobs where the physical resources are assigned by virtual machine scheduler thereby implementing resource sharing for the user jobs.

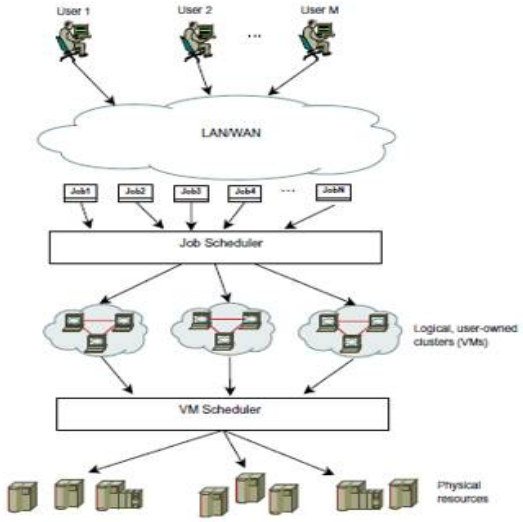

Fig 1 System Architecture

VI. IMPLEMENTATION

Implementation is one of the most important stages of system development life cycle. The stage of implementation includes converting the design phase into a real system using various programming languages and scripting languages. The implementation involves finding a stable resource allocation strategy, where the joint matching-coalition game for BSs and mobile social users is presented in Algorithm 1. The matching and coalition forming in all iterations is repeated until there is no further improve. Due to the limited number of communities and coalitions, the community will select the optimal coalition to connect and each coalition will select the optimal communities to provide resource as per the matching theory. Therefore, the given algorithm will converge to a stable result, i.e., any BS cannot improve its utility by departing from a coalition or joining a coalition.

Algorithm 1: The Matching-Coalition Algorithm

1: **Initial State**
t=0, Each coalition is one BS, which means that all BSs cannot form coalition with others. Therefore the network is portioned by F = {F1, F3, ⋯, FI}. The algorithm is used to analyze utilities of coalitions and utilities of all BSs.
2: **Repeat**
Each BS decides whether it should join a coalition or depart a coalition. The matching algorithm is used to analyze utilities of coalitions and utilities of all BSs. t=t+1;
3: **Until**
no BSs do join and departure operation to get more payoffs.

VII. RESULTS

In this section, the simulation setup is shown firstly. Then, the simulation results are given to show the performance of the joint coalition-matching game based security-aware resource allocation for mobile social big-data.

A. Simulation Setup

In the simulation, there are three BSs to provide wireless resource. Each BS has different number of mobile users where we have BS1= {1,2}, BS2 = {1,2,3}, BS3 = {1,2}. The demand degree of security resource of mobile social users is determined as required between [1, 2] represented as large or small. Further, jobs are created by users with size requirements which implies the bandwidth or wireless resource requirement. The resource status can then be obtained and sent to the scheduler for further view of tabular list of summarized input requirement from user.

B. Simulation Results

The data after being input, can then be used to calculate any overload if present. Further, the jobs entered, can obtain resources from multiple base stations using the coalition technique implementing resource sharing. The entered jobs are divided to a number of information ids to obtain more resources via resource sharing. This can then be used to obtain the report by scheduling them via scheduler. The makespan time for allocations the resources is calculated and resource utilization value is also calculated. These are then obtained as reports where efficiency and resource utilization can be viewed. Fig. 2. shows the efficiency and Fig. 3. shows the resource utilization of the simulation. It is observed that a high efficiency is obtained by using coalition technique for both wireless and security resource with smaller amount of makespan time. Comparison of results to methods such as random allocation scheme and matching scheme, shows it to be more efficient as in the matching scheme, the resource is limited in each BS, which causes the mobile social users to not obtain their satisfied demand. In the random scheme, each mobile social user obtains the amount of resource at random with the result that some resource may not be used. In the proposed scheme, BSs can form coalition to allocate resources which can satisfy the demand of mobile users.

Fig 2 Efficiency Report

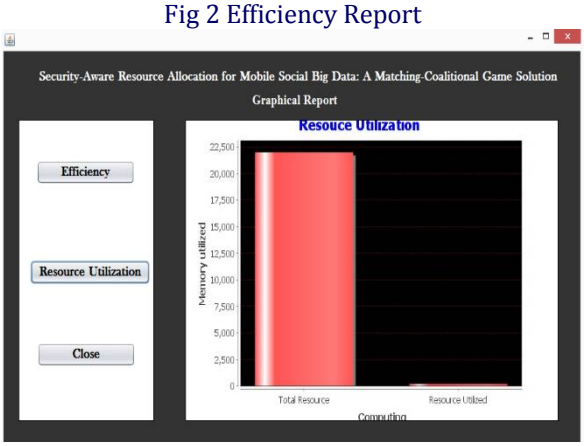

Fig 3Resource Utilization Report

VIII. CONCLUSION

This paper has presented a model based on the scheme of security-aware resource allocation based on joint coalition-matching game where both the wireless resource and security resource of the BSs can be allocated simultaneously. Specifically, based on a coalition game model, the BSs can form group to share security resource and increase resource utilization by providing these resources to mobile social users. The joint matching-coalition algorithm is introduced which can used to obtain the stable result of security-aware resource allocation. Simulation results have been presented to demonstrate the performance of the proposed model.

REFERENCES

1. S. Yu, M. Liu, W. Dou, X. Liu, and S. Zhou," Networking for Big Data: A Survey," IEEE Communications Surveys & Tutorals, vol. 19, no. 1, pp. 531-549, 2017.
2. Y. Wang, J. Wu, and W. Yang," Cloud-based multicasting with feedback in mobile social networks," IEEE Transactions on Wireless Communication, vol. 12, no. 12, pp. 6043-6053, Dec. 2013.
3. Cisco Visual Networking Index: Global mobile data traffic forecast update 2015-2020.
4. Q. Xu, Z. Su, and S. Guo," A game theoretical incentive scheme for relay selection services in mobile social networks," IEEE Transactions on Vehicular Technology, vol. 65, no. 8, pp. 6692-6702, 2016.
5. N. Kayastha, D. Niyato, P. Wang, E. Hossain," Applications, architectures, and protocol design issues for mobile social networks: a survey," in Proc. IEEE, vol. 99, no. 12, pp. 2130-2158, Dec. 2011.
6. L. Xiao, C. Xie, T. Chen, H. Dai, H. V. Poor," A Mobile Offloading Game Against Smart Attacks," IEEE Access, vol. 2016, no. 4, pp. 2281 - 2291,2016

[7] Z. Su, Q. Xu, M. Fei and M. Dong," Game theoretic resource allocation in media cloud with mobile social networks," IEEE Transactions on Multimedia, vol.18, no.8, pp. 1650-1660, 2016.

[8] J. Ren, Y. Zhamg, K. Zhang, and X. Shen," Adaptive and Channel- Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks," IEEE Transactions on Wireless Communications, vol. 15, no. 5, pp. 3718-3731, 2016.

[9] Z, Su, Q. Xu, H. Zhu, and Y. Wang," A novel design for content delivery over software defined mobile social networks," IEEE Net- work, vol. 29, no. 4, pp. 62-67. 2015.

[10] 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.

[11] M. Younis, Q. Farrag, W. Amico," Packet size optimization for increased throughput in multi-level security wireless networks," in Proc. IEEE MILCOM, pp. 1-7, 2009.

[12] J. Wang, A. Liu, T. Yan, Z. Zeng," A Resource Allocation Model Based on Double-sided Combinational Auctions for Transparent Computing," Peer-to-Peer Networking and Applications. DOI: 10.1007/s12083-017-0556-6.

