International Journal of Pure and Applied Mathematics
Volume 118 No. 20 2018, 1633-1639
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

SUSTAINABILITY OF CREDITS FOR MOBILE BASED GAMING USING BIG DATA

[1]Apoorva Kumar Dhar , [2]Sankalp Dwivedi, [3]S.Priya
[1,2]Bachelor of Technology, [3]Assistant Professor(Sr.G)
[1,2,3]Computer Science and Engineering
SRM Institute of Science and Technology Chennai - 603203, India
[1]apoorvadhar07@gmail.com,[2]dwivedi.sankalp1311@gmail.com
[3]priya.sn@ktr.srmuniv.ac.in

Abstract: As mobile user's population and proportion of networks in mobile are increasing day by day, the mobile social big data applications have become known where mobile devices are used by their users to exchange and share their data with each other. To assure mobile social big data during the delivery there is need for the security resource allocation. However, due to the limited availability of security resources, the challenge is how the security resources will be allotted. This paper is based on Joint match- coalitional game using security allocation game that is preferred by the introduction part of base station. It forms the category of security and wireless products. This resource can improve the profitability and efficiency. Secondly, a matching model is formed to determine the proceeding of selection between coalition and communities of base stations so that the users can form the community to obtain security resources. Lastly, a joint coalition algorithm is represented to form the stability of resource allocation. The experiment shows the outcome of the proposal scheme and applied schemes.

Keyword: Coalition game, Mobile networking (Social), big data and matching theory.

1. Introduction

As the communication area is increaing rapidly in today's world, the social data are being formed by many applications such as media streaming,mobile big data,etc [1]-[4].People use different kind of applications to share and exchange datas which consist of large values and volume. In the future, it is been estimated that by the year 2020 the use of mobile data will be more as compare to the year 2015. It can be stated that the usage of big data will be more in the upcoming generation[13]-[15].

The contents of data should be considered as an issue threat[16]-[18]. Taking an example, itshows that the mobile users can be tracked with their location and can even reveal what that mobile users are doing. When the mobile users are operating with the help of wireless network it should be protected by the third person.

Therefore, the computation resource is the necessity for the wireless materials. As the security of mobile big data is limited, it gives a new challenge to deliver the security for the users[19]-[26].

Although, most of the mobile networks mainly focus on various security issues instead of the security allocation. Many resources are using wireless network such as bandwidth without the usage of security. Therefore, there is alot of social big data new issues to be studied.This paper, represents the security-aware resource allocation matching with the mobile gaming coalition. The resources is been divided into two categories. Firstly, the mobile social big data is using the base station as the wireless resource provider. Secondly, it gives the guaranteed security for social activity users[30]-[31].

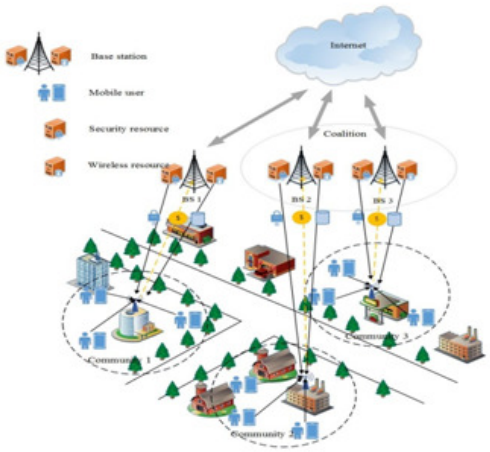


Figure 1. System Model.

The resource provides following two advantages, one is the improvement of resource sharing with the help of social data efficiency. The other part is profit that can be incremented as more redundant resources can be sold in high prices by the industries. To model group formation, coalition game analyses the process among various base station (BS).

The users with same interest from various patterns of social relations who can share the resources. The community can connect excellent players of base station which can join the preferences lists, where matching is related to the selection procedure. Moreover, we show coalition matching algorithm to have the secured formation of the security-aware resource allocation.

Contribution of the current paper represents a resource allocation of security-aware which forms the wireless resource as well as the security resource that are been joined together. The process of BSs, where sharing resources are been done to improve the efficiency and hence also increases the profits. Lastly, the coalition game solution can share the obtained solution with the given players.

2. System Model

In this section, it gives a brief explanation for mobile social networks. In addition, an example of scenario is given and the design is indicated.

Name	DESCRIPTIONS
A	Number of Base Stations
Z_i	Cost of security base station
$^{d}n;i$	n_{th} channel own by Base Station i
$\mathbf{Q}_i$	Channels own by base station
^{p}i	Wireless base station price i
$^{\Theta i}$	Resource of Price security
I	No. of communities in MSNs
I	Set of communities in MSNs
B_j	No. of user in the community j
B_j	Set of data user in the community j
$^{R}i;j$	wireless background amount in community j from BS i
$^{E}i;j$	security background amount in community j from BS i
$^{u}k;j$	Utility functions of social user $n_{k,j}$
^{e}i	Utility function of BS i
$^{p}F_l$	Cost of wireless in coalition F_l
ΘF_l	Cost of security in the coalition F_l
F	Set of coalition

3. Network Model

Mobile social networking can be considered with the following three categories:

Base station- For instance mobile social network with total of I base station (BSs). Let's assume A={1,2,3,4,5….i,…I } shows a group of base stations which gives a number of wireless resource and the resource of security for mobile users. The implementations such as monitoring and encryption can be compared with the given providers. There are two resources; one with the placing security resource in BSs that can analyze the fake users who would target and attack the network with the help of channel users. The security can give the private information with the help of algorithms. The cost price for the wireless resource depends on the rate of data while required Θ per consumption for security resource.

Communities- The mobile user is having social gathering of the communities. The social users connect BSs to download the content required for security. There are total J communities in MSNs, and set is shown as

J = {..1, 2,3,4 ….,j….,J}.

Social users using Mobile- The set of social users in community j can be formed as B={n1,n2,….nj}. The social users can form the wireless resource for connection. The energy received by interference and noise can be formed as:

$$b_{i,j,k,l} = \frac{p_i q_{i,k,l}^{m_{j,i}}}{\sum_{s \in Nj,i} p_s q_{s,k,l}^{m_{j,l}} + \sigma} \qquad (1.)$$

Where Pi is the transmission energy of the base station i, Ps is the transmission energy of base station s. The set of BSs that have similar channel d(y , i) is the noise power. The data rate produced by mobile users n (k , j) from BS 'i' can be written as:

$$b_{k,l} = \sum_{s \in L_{i,j,k}} B \log_2 1 + b_{i,s,k,l} \qquad (2)$$

Here B is bandwidth of the channel and the Q(I ,k ,j) is the set formed for the mobile user n(k ,j) in BS i.
For the resources of the security each user is having different demands. The mobile user n (k ,j) forms d (k ,j) security from the base station. The total resource in community j shows:

$$C_j = \sum_{l=1}^{M} c_{l,j} \qquad (3)$$

4. Problem Formulation

We executed a inquiry based utility function for explaining the Qality of Experience (Q o E) for the distinct users. It is a common function of sigmoid to

combine the utility function of users with varying traffic in the networks by

$$f(q) - \frac{1}{1 + e^{-q(q - q_{equ})}}$$

Where r is the amount of data received by distinct user and it is used for adjustment in slope of the utility curve around transmission rate.

r_{req} :- reflects the command amount of r_{req}. Here, the r_{req} are distant for individual users.

Security measure is required for the distinct mobile users for their common activities. Here, the security measure is achieved from BSs via hotspots.

$$f(b) = \varepsilon \log(1 + b)$$

where b is the security measure obtained. It is the satisfaction criteria for showing the inquiry amount for the mobile common users on security measure.

To improve security measure efficiency BSs can form the coalition and increment profits.

The security measure sharing problem can be formulated with following optimization problem

Problem a: $max_{q_{k,t}, b_{k,t}} u_t, t \in I$

Similarly, the problem can be formulated for the BSs as

Problem b: $max_{e} \ , j \in J$

5. Game Theoretical Plan For Security Measure Sharing

Here, the same integrated game methodology is used to eliminate two problems. Firstly, the definitions of matching theory is introduced. Then, the preference list is estimated, which is the duplicate model component. Secondly, a mutual measure sharing is introduced for the matching combination game algorithm.

5.1 The Duplicate Theory

In the duplicate model, there are bounded and disjoint set involved which are represented by X= {x1,x2,⋯ ,xi,⋯ ,xn} and Y = {y1,y2,⋯ ,yj,⋯ ,yp}, respectively. Each xi ∈ X has its individual choices above set Y and yj ∈ Y has the individual choices above the set X. The choices here is used to show rank of the opposite set to be chosen. If xi chooses y1 to y2, we represent it as y1 xi y2. Similarly, if yj chooses x1 to x2, it can be represented as x1 yj x2. It is clear that the preference of each distinctly set has full transitive properties

Definition: A duplicate μ is a one-to-many correspondence for X ∪ Y into itself. It can be expressed as function for set X∪Y into the set of X ∪ Y where we have (xi ∈ X,yj ∈ Y): 1) μ(xi) ∈ Y and |μ(xi)| =1,2) μ(xj) ∈ M ∪{∅}and|μ(xj)|∈{0,1,2,⋯ ,|X|}and 3) xi ∈ μ(yj).

We acknowledge a duplicate where the x and y are not same at value μ but can take same value at the later stage.

5.2 Preference Establishment

Algorithm 1: The demand of optimal Wireless Resource

1: Firstly, the amount of wireless resource for each and every combination is given and rate of wireless measure required. Mobile user arbitrarily chooses a wireless resource required.

2: If amount p is greater than

$$\frac{M_{i^X k,i} e^{X k,t^S equ,k,t}}{(1 + e^{X_{k,t}{}^S equ,k,t)})^2} = 0$$

3: **Else**

4: **Repeat**

6: Mobile user allocates the wireless measure required by

$$p_{k,i}(t+1) = p_{k,i}(t) + \tau \frac{\partial_{k,i}}{\partial_{k,i}(t)}$$

7. $$t = t + 1$$

8:**Until**

$$p_{k,i}(t) - p_{k,i}(t-1)/p_{k,i}(t-1)$$

9: **End Repeat**

$$p_{k,j} *= p_{k,i}(t)$$

10: **End If**

Algorithm 2: The Duplicating Algorithm

1: Firstly, every combination given rate of measures and resources to mobile users is estimated.

2: Repeat

3: All combination estimate their remaining resources and give it to each and every mobile users

4: Every association ranks the combination to choose

5: Every association chooses the first distribution to get measures for mobile user

6: Every association ranks the first distribution and assign demand to combinations

7: Every combination chooses the first distribution to associate and allocate measures for mobile user

8: till no more demand between mobile users.

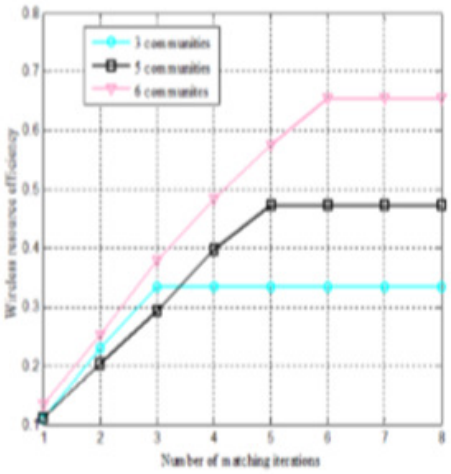


Figure 1. Wireless measure vs. the numbers of same combination iteration.

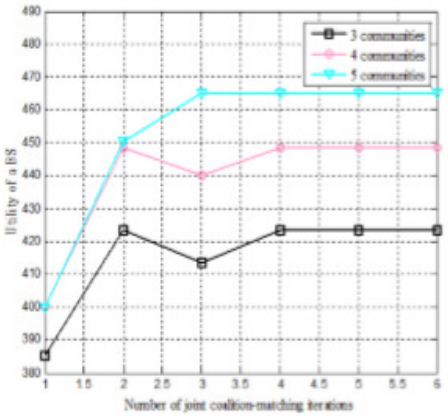


Figure 2. Security measure vs. the number of same combination iterations.

6. Performance Evaluation

From Fig. 1, we see that the efficiency of the wireless measures is decreased to optimal amount with various steps. Also, we can observe that more wireless measures can be obtained for the greater amount of communities as more mobile users desire the wireless measures. Fig. 2 represents the same combination algorithm when there is modification in the amount of communities. When the communities are 8 in amount then the security performance is fixed with 8 repetition. In the same way, the security performance with amount of communities 2 and 6 are fixed by 2 and 4 repetition respectively. In addition, since more mobile social users allocate more security resource, the high security measure performance seen for the large number of communities.

The calculation of the required security measure of a mobile user, the difference of the suggested scheme with the stable arrangements and the random arrangements is done such that. In the fixed arrangements, all users are allocated the same rate of security measure that is the total of a BS. In the random arrangement, where mobile user may not get required bandwidth then the security measures are obtained randomly. From Fig.3 We see that the arrangement is better the other suggested arrangements, where the mobile user can get more security measure than others.

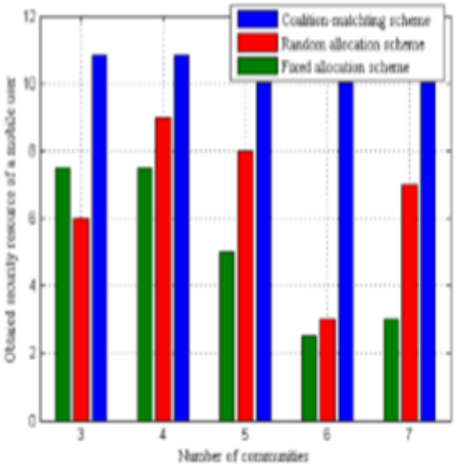


Figure 3. Obtained security resource of the number of communities.Vs mobile social user.

7. Conclusion

The paper has proposed the co-ordination of the security-ware resource allocation with the joint gaming solution. In this project, security and wireless resources of the base station can be formed parallel. Base station (BSs) can be formed to share security and analyze the total price of the resource to make the profitability according to the measure. The optimal coalition is required, where matching algorithm is used for the process of selection between coalition and mobile users. Lastly, the joint gaming solution is obtained for the required result of allocation of Security-aware resource. For the future references, we will create the security measure allocation in MSNs to deposit the base stations (BSs).

References

[1] N. Kayastha, D. Niyato, P. Wang, E. Hossain, ”Applications, archi- tectures, and protocol design issues for mobile social networks: a survey,” in Proc. IEEE, vol. 99, no. 12, pp. 2130-2158, Dec. 2011.

[2] Q. Xu, Z. Su, and S. Guo, ”A game theoretical incentive scheme for relay selection services in mobile social networks,” IEEE Transac- tions on Vehicular Technology, vol. 65, no. 8, pp. 6692-6702, 2016.

[3] 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.

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

[5] L. Xiao, D. Xu, C. Xie, N. B. Mandayam, and H. V. Poor, "Cloud Storage Defense Against Advanced Persistent Threats: A Prospect Theoretic Study," IEEE Journal on Selected Areas in Communications, 2017.DOI: 10.1109/JSAC.2017.2659418

[6] Y. Hui, Z. Su, and S.Guo, "Utility Based Data Computing Scheme to Provide Sensing Service in Internet of Things",IEEE Transactions on Emerging Topics in Computing, Jun. 2017, DOI: 10.1109/TETC.2017.2674023

[7] Q. Xu, Z. Su, K. Zhang, P Ren, and X. Shen, "Epidemic Information dissemination in mobile social networks in opportunistic links," IEEE Transactions on Emerging Topics in Computing, vol. 3, no. 3, pp. 399-409, 2015.

[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 and Q. Xu, "Content distribution over content centric mobile social network in 5G," IEEE Communication Magazine, vol. 53, no. 6, pp. 66-72, 2015.

[10] Y. Zhang, J. Ren, J. Liu, C. Xv, H. Guo, and Y. Liu, "A survey on Emerging Computing Paradigms for Big Data," Chinese Journal of Electronics, vol. 2016, no. 1, pp.1-12, 2017.

[11] 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.

[12] Cisco Visual Networking Index: Global mobile data traffic forecas- tupdate 2015-2020.

[13] Z. Su, Q. Xu, and Q. Qi, "Big data in mobile social networks: a QoE-oriented framework," IEEE Network, vol. 30, no. 1, pp. 52-57, 2016.

[14] J. Ren, Y. Zhamg, Q. Ye, K. Yang, K. Zhang, and X. Shen, "Exploit- ing Secure and Energy Efficient Collaborative Spectrum Sensing for Cognitive Radio Sensor Networks," IEEE Transactions on Wireless Communications, vol. 15, no. 10, pp. 6813-6827, 2016.

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

[16] K. Zhang, K. Yang, X. Liang, Z. Su, and X. She, "Security and privacy for mobile healthcare networks: from a quality of protection perspective," IEEE Wireless Communications, Vol. 22, No. 4, pp. 104- 112, 2015.

[17] K. Yang, K. Zhang, J. Ren, and X. Shen, "Security and privacy in mobile croudsourcing networks: challenges and opportunities," IEEE Communication Magazine, vol. 53, no. 8, pp. 75-81, 2016.

[18] C. Wu, T. Yoshinaga, Y. Ji, T. Murase, and Y. Zhang, "A rein- forcement learning-based data storage scheme for vehicular ad hoc networks," IEEE Transactions on Vehicular Technology, 2017.

[19] D. Wang, H. Cheng, D. He, and P. Wang, "On the challenges in de- signing identity-based privacy-preserving authentication schemes for mobile devices," IEEE System Journal, vol. PP, no. 99, pp. 1-10, 2016.

[20] X. Liang, K. Zhang, R. Lu, X. Lin, and X. Shen, "Fully anonymous profile matching in mobile social networks," IEEE Journal on Selected Areas in Communications, vol. 31, no. 9, pp. 641-655, 2013.

[21] S. Yu, "Big Privacy: Challenges and Opportunities of Privacy Study in the Age of Big Data" IEEE Access, vol.4, pp.2751-2763, 2016.

[22] Y. Liu, A. Liu, Y. Li, Y. Choi, H. Sekiya, and J. Li, "APMD: a fast data transmission protocol with reliability guarantee for pervasive sensing data communication," Pervasive and Mobile Computing, DOI: 10.1016/j.pmcj.2017.03.012.

[23] 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.

[24] Q. Liu and A. Liu, "On the hybrid using of unicast-broadcast in wireless sensor networks," Computer & Electrical Engineering, DOI: 10.1016/j.compeleceng.2017.03.004

[25] C. Qi, J. Wu, H. Hu, and G. Cheng, "Dynamic-scheduling mech- anism of controllers based on security policy in software-defined network," Electronic Letters, vol. 52, no. 23, pp. 1918-1920, 2016.

[26] J. Jiang, S. Wen, S. Yu, Y. Xiang, and W. Zhou, "Identifying Prop- agation Sources in Networks: State-of-the-Art and Comparative Studies," IEEE

Communication Surveys & Turials vol. PP, no. 99, pp. 1-1, 2016.

[27] 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.

[28] 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.

[29] J. Zhang, G. Pan, and H. Wang, ”On physical-layer security in un- derlay cognitive radio networks with full-duplex wireless-powered secondary system,” IEEE Access, vol. 4, pp. 3887-3893, 2016.

[30] X. Xiao, M. Li, J. Wang, and C. Qiao, Optimal resource allocation to defend against deliberate attackers in networking infrastructures, in Proceedings of IEEE INFOCOM, pp. 639-647, 2012.

[31] H. Liang, D. Huang, L. Cai, X. Shen, D. Peng, ”Resource allocation for security services in mobile cloud computing,” in Proceedings of IEEE INFOCOM, pp. 191-195, 2011.

[32] Y. Chang, H. Liu, L. Chou, and Y. Chen, et al., ”A general architec- ture of mobile social network services,” in Proceeds of. International Conference on Convergence Information Technology, Gyeongju, Korea, pp. 151-156, Nov. 2007.

[33] S.V.Manikanthan and D.Sugandhi “ Interference Alignment Techniques For Mimo Multicell Based On Relay Interference Broadcast Channel ” International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume- 7 ,Issue 1 –MARCH 2014.

[34] SHUBHANSHU GUPTA, S. KOLANGIAMMAL, T.PADMAPRIYA, “Smart Curtain Using Internet Of Things” International Innovative Research Journal of Engineering and Technology, Vol. 2, Special Issue, pp. 4-8.