Asynchronous Reputation Systems in Device-to-Device Ecosystems

Dimitris Chatzopoulos, Pan Hui
System and Media lab, The Hong Kong University of Science and Technology
{dcab, panhui}@cse.ust.hk

***Abstract*—Advances in device–to–device (D2D) ecosystems have brought on mobile applications that utilise nearby mobile devices in order to improve users' quality of experience (QoE). The interactions between the mobile devices have to be transparent to the end users and can be of many services – opportunistic networking, traffic offloading, computation offloading, cooperative streaming and P2P based k-anonymity location privacy service, to name a few. Whenever mobile users are willing to "ask for help" from their neighbours, they need to make non trivial decisions in order to maximise their utility. Current motivation approaches for mobile users that participate in such environments are of two types: (i) credit-based and (ii) reputation-based. These approaches rely either on centralised authorities or require prohibitively many messages or require tamper resistant security modules. In this paper we propose a trust-based approach that does not require synchronisation between the mobile users. Moreover, we present the three-way tradeoff between, consistency, message exchange and awareness and we conclude that our approach can provide first-rate data to neighbour selection mechanisms for D2D ecosystems with much less overhead.**

I. Introduction

Mobile cloud computing (MCC) approaches offload the most computationally expensive parts of mobile applications to cloud surrogates in order to provide better quality of experience to the end users. Advances on MCC have been mainly focused on the offloading decisions, the connectivity issues with the cloud surrogate as well as in pricing models. However, under-utilised and capable smartphones with available battery can be found nearby and their owners are willing to share their resources [1]. Nevertheless, any resource sharing has to be transparent from the end user and only needs to respect some sharing constraints. This functionality can be realised via the characteristics of the Hidden Market Design[2],[3].

Device-to-device ecosystems (D2D) are composed by mobile devices that are able to communicate without the support of any fixed infrastructure. Researchwise, D2D ecosystems are attractive due to their unpredictability, which is caused by users' mobility and the incentives required to motivate them. Given that any mobile user is self-interest and he ideally uses others' resources without sharing any of his, **cooperation enforcing mechanisms** have been proposed. Modern mobile devices are able to, not only forward each others' packets like in the traditional MANET cases, but also exchange resource-demanding services. We present four example applications in TableI. Depending on the design of the cooperation mechanism, extra processing overhead and accounting messages are needed in order to maintain and share information related to mobile users' serviceableness in the whole ecosystem.

In this work, we argue that lightweight, in terms of **(i)** message exchanging, **(ii)** processing requirements and **(iii)** storage needs, cooperation enforcing mechanisms can provide enough information to neighbour selection mechanisms (NSMs) on D2D ecosystems. In order to justify our argument we define the **price of inconsistency** as the overhead caused to the mobile users by not selecting the most suitable helpers due to lack of complete information. Additionally, we discuss the **cost of synchronisation**, which depends on **(i)** the number of the messages needed to be spread in order to inform every mobile user in the ecosystem and **(ii)** the required storage to save all the received evaluations that lead to complete information.

Neighbour selection mechanisms find the most suitable nearby users based on the score of each candidate. Our argument is based on the fact that each mobile device does not need to share all the data produced by her evaluation with others. There exists a **three-way tradeoff**, as shown in Figure 1, between the required size of data that lead to a robust estimation about nearby devices (K), the amount of data that should be broadcasted to everyone whenever two mobile users interact (N) and the freshness of the stored data (mf).

Credit based schemes stimulate user cooperation in terms of resource sharing by means of virtual currency (credits). The key idea is that users providing a service should be remunerated, while nodes receiving a service should be charged [4], [5], [6]. Reputation based schemes discourage misbehaviour by estimating users' reputation and punishing the ones with bad behaviour. The main difference between these two approaches, and also the reason we

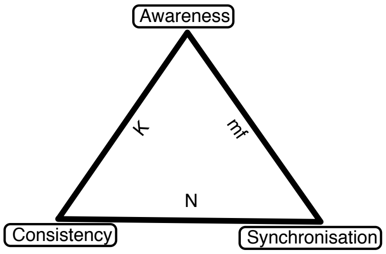


Fig. 1: Three way tradeoff of trust estimation in D2D ecosystems.

TABLE I: D2D application examples

App	**Reference**
Delay Tolerant Video Compression	[7]
Face Recognition	[8]
Cooperative Streaming	[9]
P2P based k-anonymity location privacy	[10]

decided to base our approach in a trust and reputation based system, is the fact that trust is a subjective concept since it is based on data collected by the mobile user that produces trust scores as well as from data she received by other trusted mobile users. This **subjectiveness implies a flexibility in the amount of the required message exchange and also determines the amount of inconsistency**. On the other hand, credit based systems require full consistency, otherwise any malicious user can cheat and make the system collapse. In our approach we do not force users to exchange messages after any interaction but we allow them to ask for recommendations. The frequency with which a mobile user is updating her knowledge base for other mobile users defines her **awareness**. Awareness differs from consistency on the fact that it does not require full knowledge about everything but only enough information to produce a **robust** trust score.

The concepts of wisdom of crowd and collective intelligence have been utilised by mobile application developers to create a vast spectrum of novel applications that can collectively leverage resources from other mobile devices. Applications on D2D ecosystems can be of many types. Traditional packet forwarding and routing in DTNs will regain popularity on the arrival of 5G technologies because it allows users' traffic to be routed via other proximal mobile devices. Moreover, new smartphones will be equipped with more than one cellular transceivers and will be able to connect with multiple networks at the same time. In another direction, applications will be able to be executed in more than one mobile devices [11], following the paradigm of computation offloading, that was initially proposed for MCC architectures. Table I shows four representative applications for D2D ecosystems. In the first two cases, mobile users can have better QoE because of the performance speedup and the avoidance of using MCC services that may also impose monetary costs. The cooperative streaming application is able to improve users' QoE since it provides better video quality. The k-anonymity location privacy service is used by privacy-sensitive mobile users to protect their digital footprints. The progress and the high research activity in D2D communication technologies allow mobile devices to connect via multiple ways of different range. NFC is commonly used from applications with security requirements (e.g mobile payments), WiFi-direct can work in parallel with Bluetooth, which has become more energy efficient, and also has higher coverage radius. The design of 5G, that will allow mobile traffic to pass through other mobile devices, and the invention of LTE-direct, change the way mobile devices can connect and communicate. We envision **mobile augmented reality** applications that will need mobile devices to collaborate on the virtual environment rendering and **mobile games with wearable devices** where mobile users will be connected in an ad-hoc manner and play in the cyber-physical space.

II. Asynchronous trust estimation

We consider a D2D ecosystem with a set of mobile users $\mathcal{U}$. We define as **interaction** between two mobile users the service and the message exchanges between them and we denote with N the number of the messages that were exchanged after the interaction. Any user $u \in \mathcal{U}$, at time t may need help in executing application $\mathcal{A}_u$. In this work we do not consider how u will select from whom of the other users she will ask for help. Instead, we propose a lightweight way of evaluating and bookkeeping the help of other devices. Let's assume that $\mathcal{A}_u$ is split into smaller tasks and u has decided to ask from v to help with $\mathcal{A}_u^v$. Every mobile user, via a simple interface [2], shares some of her resources. The set of shareable resources is denoted by $\mathcal{R}$ and there is a direct mapping function $r(\cdot)$ from an application vector to the set of the **minimum required resources** in order for this application to be executed properly: $r(\mathcal{A}_u^v) \rightarrow \mathcal{R}$. At the end of each interaction between mobile devices, both devices are able to evaluate the interaction. We define a history matrix on each user u for user v, $\mathcal{H}_u^v$ with values in $[0, 1]$.

We consider **recommendation** as a service, which is taking place whenever a user is sharing her experience(s) with other users. Based on the past interactions with the user that is giving the recommendations and her trustworthiness, her recommendations are evaluated. The way $\mathcal{H}_u^v$ will be used as well as the value of K depends on the cooperation enforcing mechanism. We formulate trust as a random variable $\theta_u^v(\mathcal{A}_u^v)$, which depicts how much user u trusts user v on helping her with $\mathcal{A}_u^v$. Given that $\mathcal{A}_u^v$ can be mapped to a set of minimum required resources and that u is not familiar with all interactions of v with the remaining $\mathcal{U} - \{u, v\}$ mobile users, $\theta_u^v(\mathcal{A}_u^v)$ is erroneous. Moreover, in the case where u had access to all the stored passed data with v's interactions with other users, she could have built a more robust estimation of $\theta_u^v(\mathcal{A}_u^v)$. We define $\tilde{\theta}_u^v(\mathcal{A}_u^v)$ as the trust score u could have built about v if she had access to all v's interactions ($K = \infty$). All these interaction can be known to u if the cooperation enforcing mechanism was credit based, then the enforced integrity guarantees would have allowed u to be familiar with v's interactions. On the other hand, in such a mechanism, many more messages would have been exchanged. Then the price of inconsistency is given by:

$$POI = ||\tilde{\theta}_u^v(\mathcal{A}_u^v) - \theta_u^v(\mathcal{A}_u^v)|| \tag{1}$$

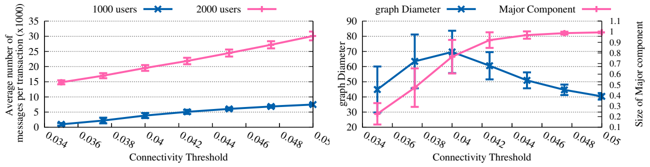
We propose a distributed approach that does not require any coordination. Our approach is based on the use of the first and second moments of $\theta_u^v(\mathcal{A}_u^v)$, which are $\mu_u^v(\mathcal{A}_u^v)$ and $\sigma_u^v(\mathcal{A}_u^v)$. In order to find out $\theta_u^v(\mathcal{A}_u^v)$ we employ Beta distribution and by calculating its parameters $\alpha_u^v(\mathcal{A}_u^v)$ and $\beta_u^v(\mathcal{A}_u^v)$ we can find its moments. $\alpha_u^v(\mathcal{A}_u^v)$ is the weighted sum of all the positive interactions u has collected about v for all cases where the services of $\mathcal{A}_u^v$ were used while $\beta_u^v(\mathcal{A}_u^v)$ is the weighted sum of the negative ones.

Any new coming mobile user does not have data for the other users. Whenever a mobile user u has in her neighbour list a candidate for help v with empty $\mathcal{H}_u^v$, she assumes that $\alpha_u^v(\mathcal{A}_u^v) = \beta_u^v(\mathcal{A}_u^v) = 1$, which gives v a trust score of 0.5 with a uniform distribution and the highest possible variance σ_u^v. We assume that every mobile user has a confidence score (i.e. maximum acceptable σ_u^v) in her opinion about other mobile users and in order to satisfy this confidence score she requests information about others from other trusted friends.

Given that the information that is produced by our proposal is going to be used by NSMs that are targeting on improving the QoE of D2D applications, it is important to not marginalise mobile users for their selfish attitude in the past. On the other hand, free riders should not have the same confrontation as the altruists. During the calculation of $\alpha_u^v(\mathcal{A}_u^v)$ and $\beta_u^v(\mathcal{A}_u^v)$, we use a multiplication factor on each entry i of $\mathcal{H}_u^v$: $mf = \frac{\lambda}{t-t_i}$. where λ is a possitive tuning parameter, t is the current timestamp and t_i the timestamp that the entry i was collected. mf slows down the decrease of the variance and feeds the need for new entries. In the general case, any mobile user requests for others' recommendation whenever her current evaluation has bigger variance that the imposed threshold. If her current entries is less than K, she just enters more entries in her history matrix. If her history matrix is full, she discards entries with small contribution to the distribution.

III. Evaluation

We show the validity of our initial argument via an analysis of users that are uniformly distributed and we show how their population size and the connectivity between them affects the number of the messages needed to maintain the integrity of a credit based system. We produce instances of static Random Geometric Graphs using MATLAB. We distribute uniformly users in a $[0, 1] \times [0, 1]$ area. In Figure 2a we show how many retransmissions are required in order for one message to arrive to all the users of the network in the case of 1000 users or 2000 users. The x-axis of both figures 2a and 2b show the connectivity threshold. By connectivity threshold we define the ratio between the coverage radius of a smartphone to the whole examined area. Moreover, Figure 2b shows how the graph diameter is decreasing and the fraction of the users in the major connected component is converging to 100% when the connectivity threshold is increasing.



(a) (b)

Fig. 2: Transmitted messages per transaction (left) and Graph diameter and size of the major connected component (right) for different values of the coverage area

IV. Acknowledgements

This research has been supported by the General Research Fund 26211515 from the Research Grants Council of Hong Kong and the Innovation and Technology Fund ITS/369/14FP from the Hong Kong Innovation and Technology Commission.

References

[1] C. Bermejo, R. Zheng, and P. Hui, "An empirical study of human altruistic behaviors in opportunistic networks," in *Proceedings of the 7th International Workshop on Hot Topics in Planet-scale mObile computing and online Social neTworking*. ACM, 2015, pp. 43–48.

[2] S. Seuken, D. C. Parkes, E. Horvitz, K. Jain, M. Czerwinski, and D. Tan, "Market user interface design," in *Proceedings of the 13th ACM Conference on Electronic Commerce*. ACM, 2012, pp. 898–915.

[3] D. Chatzopoulos, P. Hui, and D. Huang, "Fides: A hidden market approach for trusted mobile ambient computing," in *Computer Communications Workshops (INFOCOM WKSHPS), 2015 IEEE Conference on*, April 2015, pp. 81–82.

[4] L. Buttyán and J.-P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," *Mob. Netw. Appl.*, vol. 8, no. 5, pp. 579–592, Oct. 2003.

[5] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol," in *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*. ACM, 2002, pp. 226–236.

[6] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Advanced communications and multimedia security*. Springer, 2002, pp. 107–121.

[7] D. Chatzopoulos, K. Sucipto, S. Kosta, and P. Hui, "Video compression in the neighborhood: An opportunistic approach," in *Communications (ICC), 2016 IEEE International Conference on*, 2016, p. to appear.

[8] R. Kemp, N. Palmer, T. Kielmann, and H. Bal, *Mobile Computing, Applications, and Services: Second International ICST Conference, MobiCASE 2010, Santa Clara, CA, USA, October 25-28, 2010, Revised Selected Papers*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, ch. Cuckoo: A Computation Offloading Framework for Smartphones, pp. 59–79.

[9] L. Keller, A. Le, B. Cici, H. Seferoglu, C. Fragouli, and A. Markopoulou, "Microcast: Cooperative video streaming on smartphones," in *Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '12. New York, NY, USA: ACM, 2012, pp. 57–70.

[10] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46–55, Jan 2003.

[11] C. Shi, V. Lakafosis, M. H. Ammar, and E. W. Zegura, "Serendipity: Enabling remote computing among intermittently connected mobile devices," in *Proceedings of the Thirteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, ser. MobiHoc '12. New York, NY, USA: ACM, 2012, pp. 145–154.