Exploiting 4G Mobile User Cooperation for Energy Conservation: Challenges and Opportunities

Bechir Hamdaoui, Tamara Alshammari, and Mohsen Guizani†
Oregon State University, Email: hamdaoub,alshamta@onid.orst.edu
† Qatar University, Email: mguizani@ieee.org

***Abstract*—Recent years have witnessed tremendous success and popularity of mobile applications and services, resulting in an explosive growth in the number of mobile devices, as well as in the range and types of things these devices can do. People nowadays become extremely dependent on their smartphones and handheld devices to access and receive online services. While computing and processing powers of these handheld devices are keeping up with this demand, battery lifetime remains the performance bottleneck, and researchers are now more challenged than ever before to come up with new techniques that can make efficient use of the devices' energy resources. In this article, we focus on exploiting user cooperation as a way of conserving energy in 4G mobile networks. We first begin by overviewing user cooperation and illustrating its potential for reducing energy consumption. Then, we describe the key challenges 4G mobile users face vis-a-vis of cooperation. Finally, we discuss some of the techniques proposed in literature to address these challenges by highlighting their methodologies, advantages, and disadvantages.**

***Index Terms*—Cooperative networking, energy efficiency, mobile 4G networks.**

I. The Mobile Internet Era

With the recent, fast-growing popularity of mobile applications and online services, the number of mobile handheld devices has recently been increasing at explosive rates. Cisco's recent studies forecast that the number of mobile-connected devices will exceed the number of people on earth by the end of 2013, and that this number is projected to reach about 10 billion by 2017, which is about 1.4 mobile device per capita [1]. Not only are these mobile devices reaching billions and billions of people, but they are also becoming more and more capable of performing all sorts of tasks and applications, ranging from watching videos and live games via real-time streaming to locating favorite restaurants via GPS, and from making an e-payment for online shopping to keeping up with friends via Facebook. Mobile data traffic is forecasted to increase 13-fold between 2012 and 2017 [1]. In brief, we are, without any doubt, witnessing a major technological cycle–The mobile Internet service era.

Alongside this unprecedented growth of mobile data traffic, recent years have also witnessed the emergence of several, new service and user behavioral trends.

Mobility. The number of 4G mobile users has increased dramatically, and is expected to double by 2016 [2]. Studies, for example, show that 73% of Italians prefer to use their smartphones to access Internet over their home computers even when they are at home [3]. Clearly, mobility nowadays is no longer a luxury, it is becoming a necessity.

Dependence. Another trend that has also been noticed is the increased reliance and dependence on mobile Internet applications and services. Studies show that more than 50% of users use their smartphones, on a daily basis, to check emails, access Facebook accounts, browse Internet, and check bank and other personal accounts [4]. Users are becoming, more than ever, highly dependent on online Internet services, such as e-shopping, location-based services, real-time streaming, gaming, Googling, e-reading, etc.

Always-on. Having continued access and connectivity to network services wirelessly is also another trend and luxury that users do not seem to be willing to give up. For example, studies show that more than several times a day, smartphones are used by 64% of users for texting, 40% of users for browsing Internet, and 35% of users for Facebook [4]. Nowadays, users expect to be and stay connected and receive network services anytime and anywhere.

All-in-one. Users now expect their handheld mobile devices to do it all for them. They indeed use their mobile devices for shopping (m-commerce, e-payment, etc.), entertainment (gaming, streaming, blogging, etc.), networking (social media, Facebook, etc.), traveling (GPS, camera, etc), and for work too (emailing, browsing, voice, etc.). ExactTarget [4] says it nicely:

> *The smartphone has become a modern day Swiss Army knife, putting marketers not only in a multichannel environment, but a multipurpose environment as well.*

Fortunately, technology is keeping up with the users' needs and expectations, and is indeed turning smartphones into modern day Swiss Army Knives.

These above trends share and give rise to one key challenge that next-generation mobile devices ought to carefully address to meet these users' expectations and demands: availability of energy resources. If this challenge is not promptly addressed, mobile users will more likely end up searching for power outlets than for network connections. Therefore, our focus in this article is on the energy conservation problem that 4G mobile devices face. Specifically, we focus on the exploitation of user cooperation to make effective use of available energy resources.

We first begin by overviewing user cooperation, illustrating its potential for reducing energy consumption, and describing the key challenges 4G mobile users face vis-a-vis of cooperation. Then, we overview some of the proposed techniques to address these challenges by highlighting their

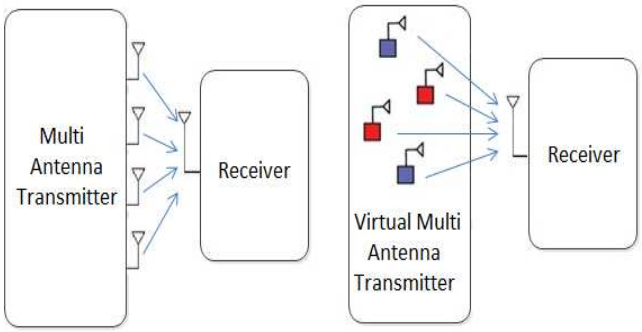

Fig. 1: Channel diversity

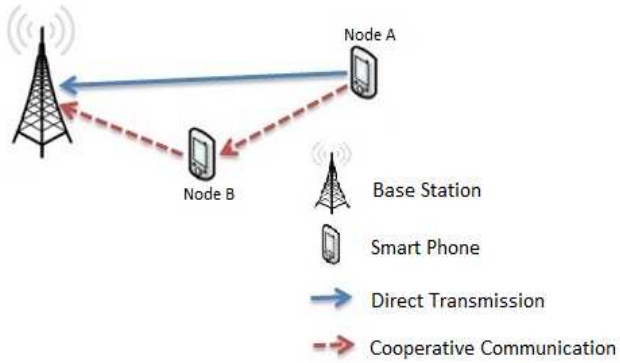

Fig. 2: User cooperation

methodologies, advantages, and disadvantages. Finally, we conclude the article.

II. User Cooperation and Energy Conservation

The idea of using cooperation to improve performance traces its roots back to the work of van der Meulen in 1968, where relaying is used for combatting fading via channel diversity. Single-antenna equipped mobile users can then cooperate by offering to use their antennas to create virtual multiple antenna systems to mimic transmit diversity, without requiring nodes to be equipped with multiple antennas. This is illustrated in Figure 1.

Cooperation can also be used by mobile users to simply forward or relay each other's data instead of being used to improve channel quality. Unlike the case of channel diversity where cooperation is mainly used to improve the channel quality, user cooperation is a way for users to help one another by relaying each other's data. Taking Figure 2 as an example, if node A is far away from the base station (or the channel between it and the base station is poor), then it may send its data to node B which will then relay it to the base station. Another great benefit of user cooperation is power conservation; the total amount of energy needed to send A's data directly to the base station may be much greater than the total energy to be needed when using cooperation. Another scenario where cooperation can be beneficial is when a node's battery is running low. In this case, a node can rely on a nearby node whose battery is full (er) to relay its data.

Clearly, user cooperation has great potential for reducing energy consumption of mobile users. However, one key challenge that needs to be overcome is users' willingness to cooperate, which is perhaps the most challenging problem when it comes to user cooperation. There are multiple reasons for why users may not be willing to cooperate. One reason could be because users may not see an immediate benefit and reward of their cooperation. Two, users may have some security and privacy concerns. A third reason could be resource limitation. For e.g., users may not be willing to drain their batteries for the sake of forwarding other users' traffic. A forth reason that might discourage users from relaying is misbehavior, as some users may be selfish, malicious, or even hackers. A selfish user is one that receives help from other users to relay its traffic but it refuses to help others when asked to do so. Such selfish behavior can degrade the system performance and can lead to unfairness. Malicious users are those that take advantage of cooperation to damage network operation and/or intercept transmitted data.

Three essential elements that need to be supported in order to promote user cooperation: incentive mechanisms, enforcement strategies, and relay selection approaches.

III. Incentive Mechanisms

Users cannot be forced to cooperate, nor should they be. Cooperation can only be at their will, and hence it can only be encouraged. As mentioned earlier, there are indeed legitimate reasons that make users shy away from cooperation, and the only way through which cooperation can be promoted is by giving users good incentives to do so.

Several incentive mechanisms have been proposed in recent years in an effort to encourage users to cooperate [5–7]. Some mechanisms treat the packet-forwarding/relaying task as a service. When the source user or node[1] communicates with the destination node through intermediate nodes (relays), the relays will be rewarded for their help, and the source, destination, or both will be charged for the service. The charging/rewarding is done by exchanging virtual currency or credit among nodes, which is converted later to either real money or some form of service.

An important question arises here is how and when does charging/rewarding happen? Here are several approaches that are proposed to answer this question.

Cost paid by source node. The first approach requires that the source node loads the packet to be forwarded with a sufficient amount of virtual currency before sending it to the destination [5]. During packet transmission, each intermediate node (relay) deducts some of the uploaded virtual currency as a reward for forwarding the packet. This approach requires temper-proof hardware, which is needed to enable the deduction of the virtual currency that is being transmitted along with the packet. Furthermore, in this approach, the source node is the only node that is charged for the cost

[1]Node and user will be used interchangeably throughout.

of cooperation. An advantage of this is that it can reduce the risk of attacks by malicious nodes. This, however, can be unfair, as the source only ends up paying all the cost of the communication; the destination node does not get charged.

Cost paid by destination node. The second approach requires that each intermediate node buys the packet from the previous node for some amount of virtual currency, and sells it to the next node for a higher amount [5]. Here, the destination node is the only node that pays the forwarding cost. Unlike the previous approach, this approach increases the risk of malicious attacks; for e.g., malicious nodes can transmit a large number of packets just to charge the destination node. Also, this approach is unfair to the destination node, as it has to pay all the forwarding cost.

Cost paid by virtual bank. Another approach requires a third-party that is trusted by all the nodes; e.g., a virtual bank or clearance center [6]. When an intermediate node receives a packet and forwards it, the node keeps a signed receipt (check) of the packet and later submits it to the clearance center. This signed receipt is generated by the source, and signed with the source's secret key and appended to the packet that will be forwarded. When the clearance center receives the receipt, it charges the source node, and rewards the intermediate nodes. In some cases, both of the source and destination nodes are charged, and thus both of them must sign the generated check. Here, when both source and destination nodes are charged, a fair charging policy is achieved. However, this could open up the door for some malicious attacks and behaviors. For example, the source node may collude with the intermediate nodes in order to reduce the total amount of virtual currency that the source has to pay, making the destination node pay more.

An alternative approach aiming to reduce the payment overhead is to generate a small-sized check per route instead of generating a check for each intermediate node [6]. This small-sized check contains all the payment information for all the intermediate nodes that were involved in the routing path. For this, the submitting methodology depends on the communication mode; i.e., whether it operates in a hybrid mode or in a pure ad hoc mode. A hybrid mode means that at least one base station is involved in the communication, whereas a pure ad hoc mode means that the nodes are communicating without needing base stations. In the hybrid mode, the base station is responsible for submitting the check to the clearance center, whereas in the ad hoc mode, it is the job of the intermediate nodes to do so. However, it is insecure to have one node submit all the checks that contain all the payment information for all the cooperative intermediate nodes, as this submitter node may collude with the source, destination, or both to avoid submitting the check to the clearance center, thus preventing the other intermediate nodes from taking any credit. It is therefore necessary to come up with alternative methodologies that eliminate this threat. One of the proposed methods suggests to let one node submit the check, but instead of fixing this node all the time, the node can be changed randomly according to a public function that is executed by all the intermediate nodes that were involved in the communication. This could reduce the risk; hence neither the source node, nor the destination node will know which intermediate node is going to submit the check.

IV. Enforcement Strategies

Incentive mechanisms are necessary for promoting cooperation, but they are not sufficient. One should also make sure that selfish behaviors are penalized, where selfishness refers to the case when users seek and receive relaying service from other users, but refrain from offering theirs to others. Therefore, cooperation enforcement strategies are to be developed and adopted in order to tackle (and hopefully prevent) selfishness and maliciousness.

A common strategy used to enforce user cooperation is to rely on reputation to identify selfish nodes in the network [5, 8]. In other words, nodes that show a low reputation value (RV) are considered as misbehaved nodes. These misbehaved nodes will be isolated and removed from the list of cooperative users; i.e., deprived from the relaying services.

The RV of a node increases when the node carries out the forwarding service properly. That is, every time a node performs the cooperative task as expected, its RV is incremented. But when a node does not do so as expected, its RV is decremented, and does so until it reaches a predefined threshold. Once the RV of a node reaches this threshold, the node will be isolated from the user cooperative list; i.e., the node's relaying service privilege is removed. While some mechanisms consider this as a final decision, others give the node a second chance (second chance mechanisms) by restoring the cooperation privilege back to the node. In these mechanisms, after some amount of time, a misbehaved node can join the list again, but with a very low RV to guarantee that it will go back quickly to the black list if it starts misbehaving again. Also, whenever a new node joins the list, it will be assigned a small RV in order to stimulate it to do its best to cooperate.

A node can either depend on only its neighbors' reputation observations (first-hand reputation), or also use the observations of other nodes in the network (second-hand reputation). These two approaches are discussed next.

First-hand reputation. Each node has a monitor (or a watchdog) that detects misbehaved nodes by listening to the neighbors' transmissions [5]. Its purpose is to make sure that the next neighboring node does the forwarding task properly, and if it does not do so, the neighboring node is considered as a misbehaved node. The main drawback of this scheme is that each node has to maintain a reputation value of each of its neighbors, thus incurring more overhead.

Second-hand reputation. Nodes exchange information with one another, and if a node observes that another node does not carry out the forwarding task rightly, it reports this misbehavior to the rest of network [8]. Generally speaking, each node here maintains three structures: trust table, alarm table, and friend list. The alarm table contains the alarms that the node receives from other nodes. The trust table

is used to determine the trustworthiness of the alarm. For example, if node A sends an alarm message to node B indicating that node C is a malicious node, then the trust table in node B is used to determine how much node B trusts node A to decide whether to accept and consider the alarm message as legitimate. In other words, the trust rating is used to decide whether to accept the indirect reputation messages or alarms from a node. The friend list contains all the friends that the node will send alarm messages to when it detects any misbehaved node. However, friendship relations are asymmetric in that a node may consider another as a friend, but not vise-versa.

Some reputation strategies do not support the second-hand reputation exchanges for the following reasons. Each node has to maintain an RV of every other node in the network, thus increasing the amount of needed storage. Also, network traffic increases as a result of the exchange of RVs among nodes. In addition, when a node receives indirect reputation information, it has to decide whether to accept it, leading to an increase in the computation at each node. On the other hand, reputation strategies that support the use of second-hand reputation argue that it detects selfish and malicious nodes faster.

Generally speaking, the RV of a node is not an accurate measure of how well the node behaves. This is due to the fact that smartphone users are humans, and humans are not expected to always have the same behavior. Furthermore, reputation-based strategies do not achieve fairness. For instance, if a node does not have enough resources (e.g., its battery is running low), it may be considered as a selfish node if it chooses not to cooperate. This node might be isolated from the network due to not being able to help out, which is unfair, as this unwillingness is due to the lack of resources, and not due to its selfishness.

V. Relay Selection Approaches

The previous two sections discussed incentive mechanisms and enforcement strategies, both required to promote user cooperation. In this section, we go through another equally important element also needed for promoting cooperation: relay selection. The question is how and how many relaying nodes should be selected when cooperation is needed?

Several approaches have been proposed in the literature to select the best relay(s). Generally speaking, relays could be categorized into three classes: dedicated-fixed relays, dedicated-mobile relays (e.g., a mobile node placed at the top of a train), and non-dedicated users (e.g., smartphone). In this article, we focus on the latter class of relays whose selection approaches can be categorized into two categories: single-relay selection and multiple-relay selection.

Single-relay selection approaches aim to find the best relay node that meets certain performance criteria.

- Best relay node selection: selects the relay node that yields the maximum received SINR [9].
- Best worst channel selection: recall that each relay has two channels: source-to-relay and relay-to-destination channels. This approach finds the worst channel among the above two for each relay node, and then selects the relay node that has the best worst channel [10].
- Best harmonic mean selection: selects the relay node that has the largest harmonic mean [10].
- Nearest neighbor selection: selects the relay node that is the nearest to the base station [9].
- Contention based selection: the source node first sends a message to all relay nodes, and those relays that could decode the message send a "Hello" message back to it. At the end of this contention period, the source node selects randomly one of the relay nodes whose "Hello" messages were received successfully [11].
- Least energy cost selection: selects the relay node that can perform the forwarding task with the least energy cost [12].
- Least remaining energy selection: chooses the relay whose cooperative task results in the highest amount of remaining battery level (i.e., after performing the forwarding task) [12]. This approach ensures that the user, after cooperation, still has a sufficient amount of energy, as one of the key reasons for users' unwillingness to cooperate is energy concerns.

Multiple-relay selection approaches aim to find a set of relay nodes that best meets certain performance criteria. The same performance metrics used for single-relay selection can also be used here. The following are few examples.

- SINR: When taking SINR as a performance metric, multiple-relay selection approaches aim then to find a set of nodes that result in the best received SINR. Note that an exhaustive search may be required to find the path with the maximum SINR, making this approach somewhat complex. To address this, some researchers proposed to decrease the number of the operations required to find the best path by first ordering the relay nodes according to an optimal relay ordering function [9], and then searching for the best path.
- Transmission time. Another performance metric is to select the set of nodes that reduce the total transmission time [13]. Here, the number of relay nodes can be fixed a priori or determined adaptively. It can be determined adaptively so as to adjust to the network conditions in realtime; for e.g., select the relay nodes that provide the best source-to-relay channel in realtime.
- Task distribution. Other approaches distribute the forwarding tasks among available relays so that all devices spend the same amount of energy when executing these tasks [12]. This appears to be fair, but determining how much energy each task consumes can be challenging.

Multiple-relay vs. single-relay selection. We now present simulation results, comparing and contrasting multiple- and single-relay selection approaches. In this simulation study, we consider a simple network with one pair of source-destination nodes, and three relays (all assumed to be willing to cooperate). Each relay has two channels, source-relay and relay-destination, both assumed to be i.i.d. complex Gaussian

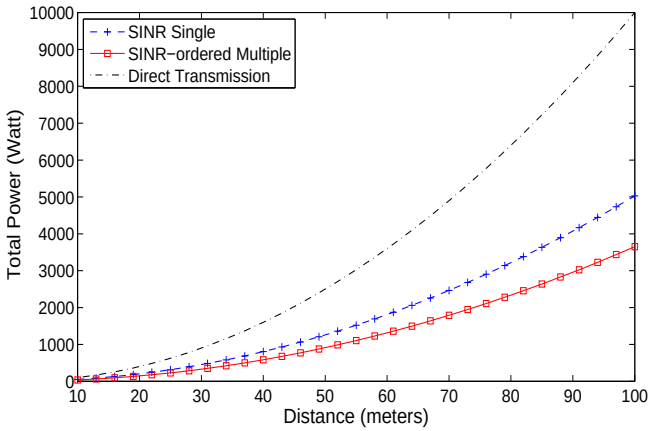

Fig. 3: Total consumed power as a function of distance.

random variables with zero-mean and unit-variance. The distance between the source and the destination nodes is varied during the course of simulation, and the relays are placed randomly. In Figure 3, we show the total consumed energy as a function of the distance between the source and the destination for three relay selection approaches: single relay with best SINR (referred to "SINR single" in the figure), multiple relays with best received SINR (referred to "SINR ordered multiple" in the figure), and no relaying (referred to as "Direct Transmission" in the figure).

Simulations show that regardless of the relay selection approach (i.e., whether single or multiple relay), cooperation always (in our simulated topology) conserves power when compared to direct transmission (i.e., without cooperation). Also, the power savings increase with the distance, and it is more pronounced for the multiple relay approach than for the single relay one. We want to mention that this simulation setup is very simple and does not account for communication/coordination overhead; it just considers energy savings.

VI. Beyond Cooperative Communication

We have so far discussed users' cooperation in the context of relaying/forwarding each other's traffic; i.e., communication cooperation. Cooperation, however, can go beyond just data forwarding. Cooperation can encompass other forms of tasks, such as storage and computation.

Nowadays, smartphones have powerful computational resources that can be used to cooperatively run sophisticated applications [12, 14, 15]. This can be referred to as cooperative computation. Here, each smartphone is considered as a single processing unit, and the overall environment is considered as a multi-processor environment. The computational task is then to be divided among all the nodes that are willing to cooperate. These selected nodes will exchange information among themselves using short range wireless networking. It is important, in such cases, to have a monitor component to respond to dynamic changes in application requirements and in network topologies, such as node mobility or failure.

Two important components are needed in order to promote task computation distribution: efficient schedulers, to distribute tasks among the nodes, and energy-efficient techniques, to reduce the overall amount of consumed energy (dynamic voltage scaling (DVS) [15] is an example).

VII. Conclusion and Future Work

We discussed challenges and opportunities that user cooperation brings to 4G mobile users, with a special focus on energy consumption. We stated some of the reasons for users' unwillingness to cooperate and discussed the challenges cooperation faces. We also described the key components cooperative networks ought to have to promote cooperation, and highlighted their advantages and disadvantages.

Although these proposed cooperation techniques aimed at improving the network performance in terms signal quality and packet throughput, little has been done towards energy efficiency. Energy-aware technique development is still in its infancy. Another challenge that also needs to be paid a close attention to when designing such cooperation techniques is security. Although attempts have been made to address security, a comprehensive framework that targets security and energy awareness at the same time is still an open problem.

VIII. Acknowledgment

This work was made possible by NPRP grant # NPRP 5-319-2-121 from the Qatar National Research Fund (a member of Qatar Foundation) and by NSF grant # 1162296 from the National Science Foundation. The statements made herein are solely the responsibility of the authors.

References

[1] Cisco. Cisco visual networking index: Global mobile data traffic forecast update. February 2013.

[2] iETSolutions. http://www.iet-solutions.com, last visited in April 2013.

[3] C. Jayawardhena and K. Korsah. Mobile economic time. *www.brandchannel.com/images/papers/531_ca_technologies_wp_mobile_economic_time_0911.pdf*.

[4] Mobile dependence day. *http://www.exacttarget.com/Resources/SFF9_web.pdf*.

[5] J. Hu and M. Burmester. In *Guide to Wireless Ad Hoc Networks*, chapter Cooperatin in Mobile Ad Hoc Networks. Springer, 2009.

[6] M. Mahmoud and X. Shen. Fescim: Fair, efficient, and secure cooperation incentive mechanism for multihop cellular networks. *IEEE Transactions on Mobile Computing*, 11(5):1536–1233, May 2012.

[7] D. Yang, X. Fang, and G. Xue. Game theory in cooperative communication. *IEEE Wireless Communications*, 19:44 – 49, April 2012.

[8] G. Bella, G. Costantino, , and S. Riccobene. Evaluating the device reputation through full observation in manets. *J. Information Assurance and Security*, 4(5):458–465, March 2009.

[9] Y. Jing and H. Jafarkhani. Single and multiple relay selection schemes and their achievable diversity orders. *IEEE Transactions on Wireless Communications*, 8(3):1414–1423, March 2009.

[10] A. Bletsas, A. Khisti, D.P. Reed, and A. Lippman. A simple cooperative diversity method based on network path selection. *IEEE J. Select. Areas Commun.*, 24:659–672, March 2006.

[11] C.K. Lo, S. Vishwanath, and Jr. R.W. Heath. Relay subset selection in wireless networks using partial decode-and-forward transmission. *IEEE VTC-Spring*, May 2008.

[12] J. Furthmuller and O. P. Waldhorst. Energy-aware resource sharing with mobile devices. *Computer Networks Journal*, pages 1920–1934, 2012.

[13] S. Nam, M. Vu, and V. Tarokh. Relay selection methods for wireless cooperative communications. *Information Sciences and Systems*, pages 859–864, March 2008.

[14] B. Seshasayee, R. Nathuji, and K. Schwan. Energy-aware mobile service overlays: Cooperative dynamic power management in distributed mobile systems. *International Conference on Autonomic Computing*, 2007.

[15] A. B. Olsen, F. Fitzek, and P. Koch. Evaluation of cooperative task computing for energy aware wireless networks. *in Proc. International Workshop on Wireless Ad-Hoc Networking (IWWAN)*, 2005.