Incentive Mechanisms in Multi-Hop Wireless Networks

Levente Buttyan, Markus Jakobsson, Jean-Pierre Hubaux, Naouel Ben Salem

Incentive Mechanisms in Multi-Hop Wireless Networks

Levente Buttyán[1] Markus Jakobsson[2] Jean-Pierre Hubaux[1] Naouel Ben Salem[1]
[1] Laboratory for Computer Communications and Applications
Swiss Federal Institute of Technology – Lausanne (EPFL), Switzerland
[2] RSA Laboratories, Hoboken, NJ, USA

1 Introduction

In multi-hop wireless networks, data packets are relayed in several wireless hops from their source to their destination. Based on whether a fixed infrastructure is used or not, we can distinguish two types of multi-hop wireless networks: pure ad hoc and multi-hop cellular networks. Pure ad hoc networks do not rely on any fixed infrastructure; hence, the packet relaying service has to be provided solely by the end user devices. Multi-hop cellular networks rely on a set of base stations that are connected to a high speed backbone network; here, data packets have to be relayed by end user devices from the source to the backbone and from the backbone to the destination. Multi-hop cellular networks are a potential evolution of both voice-centric networks such as GSM and data-centric networks such as CDPD or IEEE 802.11.

The proper operation of both types of network requires the end users to collaborate. However, collaboration is not individually beneficial for the users, because it consumes resources such as battery power, memory, and CPU cycles, and it does not provide any immediate advantages (serving others does not guarantee for the user that he will be served as well). Indeed, if the majority of the users collaborate, a selfish user can parasitically take advantage of this by using the network without contributing to it.

While the problem is the same in both pure ad hoc and multi-hop cellular networks, the solutions can be very different. This difference mainly stems from the different set of assumptions that can be made in the two cases. In particular, in multi-hop cellular networks, the operator(s) of the backbone can be considered as a trusted authority, which can – at least to some extent – control the operation of the network by implementing various security measures, while in pure ad hoc networks, the existence of such a trusted authority cannot be assumed.

In this paper, we present our ongoing work on the design of mechanisms that stimulate collaboration of end users in both pure ad hoc and multi-hop cellular networks. We put the emphasis on stimulating packet forwarding, as this is one of the most fundamental services that end users should provide to each other.

2 Stimulating packet forwarding in pure ad hoc networks

The absence of a trusted authority that can control the operation of the network makes stimulation of collaboration among nodes in pure ad hoc networks a very challenging problem. Our approach [2] is based on the notion of tamper resistance. One solution in this vein would be to program the correct (collaborative) behavior in tamper resistant end user devices. However, this does not seem to be very realistic, since ensuring that the whole device is tamper resistant may be very difficult, if not impossible. Therefore, we propose another approach that requires only a tamper resistant hardware module (such as the SIM card in GSM phones) in each device. We call this tamper resistant module the *security module*. Our assumption is that the user cannot modify the behavior of the security module. In addition, while tampering with the rest of the device is possible, our design ensures that the user cannot gain any advantages by doing so.

We propose an incentive mechanism for packet forwarding that relies on the security module. The proposed mechanism is based on a protocol that requires the device to pass each packet (generated as well as received for forwarding) to its security module. The security module maintains a counter, called *nuglet counter*. When the device wants to send a packet as originator, the number n of relaying nodes that are needed to reach the destination is estimated, and the nuglet counter is decreased by n. On the other hand, when the device forwards a packet, its nuglet counter is increased by one. The value of the nuglet counter must remain positive (a property enforced by the security module), which means that the device can send its own packets only if it forwards packets of the others.

We study the behavior of the proposed mechanism by means of simulations. In our simulations, each node generates packets with a constant average rate. We assume that if an own packet cannot be sent (due to the low value of the nuglet counter), then it must be dropped, and we model the selfishness of the nodes by the goal of minimizing the number of own packets dropped. We study the performance of several heuristic packet forwarding strategies under the above assumption. The simulation results show that more cooperative strategies achieve higher performance, which means that the proposed mechanism indeed stimulates collaboration.

3 Stimulating packet forwarding in multi-hop cellular networks

As we mentioned in Section 1, mechanisms to stimulate collaboration in multi-hop cellular networks can take advantage of the presence of the backbone network operator(s). It is reasonable to assume that the operator(s) is trusted. This makes it possible to implement currency-based stimulation mechanisms like the one proposed in the previous section, but without relying on tamper resistant hardware.

In the following, we assume a multi-hop cellular network that supports multi-hop up-stream and single-hop down-stream communications; we call this type of network an *asymmetric* multi-hop cellular network. While this model is different from the one usually considered for multi-hop cellular networks [4], it has certain benefits that make it worthwhile to consider. We propose an exceptionally light-weight micro-payment scheme for such asymmetric multi-hop cellular networks that stimulates packet forwarding by letting users benefit from forwarding others' packets. Besides detecting and rewarding collaboration, our scheme also contains mechanisms for detecting and punishing various forms of abuse.

In the proposed system [3], each packet is accompanied by a payment token computed by the source of the packet. Each relaying node on the path from the source to the base station verifies if this token corresponds to a *winning ticket* for him. Winning tickets are reported to nearby base stations at regular intervals, and they are forwarded to an accounting center. After verifying the validity of the payment tokens, the base stations send the packets (now without their corresponding payment tokens) to their intended destinations over the backbone network. Packets with invalid tokens are dropped, as the transmission of these cannot be charged to anybody. The base stations also send the payment tokens (or some fraction of these and potentially in batches) received in the packets to the accounting center.

Sources are charged after their packets that reach the base stations, and relaying nodes are rewarded after the winning tickets that they report. Therefore, instead of using one payment token per payee (as is done in traditional micro-payment schemes), we, in fact, use one *per packet*. To avoid forged deposits, the source of the packet needs a secret key to produce the token (not unlike in other payment schemes). To discourage colluders from collecting payments for each other, we require the intermediary's secret key (the same as is used to request service) to be used to verify whether a ticket wins. Thus, mutually suspicious colluders will not give each other their secret keys, as this would allow the others to request service billed to the key owner.

In addition, a relaying node profits not only from its own winning tickets, but also from those of its neighbors: Each relaying node with a winning ticket is required to report the identities of its neighbors along the packet's path when filing a reward claim, and these neighbors are also rewarded. This has three direct benefits: First, the "neighbor reward" encourages the *transmission* of packets (even if they carry losing tickets, as they may be winning for the next hop neighbor), while the "personal reward" can be seen as a reward for *receiving* the packet and for reporting this to the accounting center. Second, it increases the number of rewards per deposited ticket, which in turn means that fewer tickets need to be deposited. Third, and more importantly, it allows for the compilation of packet forwarding statistics that can be used to detect inconsistent (cheating) behavior of relaying nodes. By comparing the relative amounts of "neighbor rewards" and "personal rewards" on a per-node basis, the accounting center can detect various forms of abuse. In particular, this analysis will identify parties that routinely drop packets, and parties that refuse to handle packets without winning tickets. It will also detect various forms of collusion. While the auditing techniques only detect *repeated* misbehavior (as opposed to the very occasional abuse), this is sufficient, as very few users are likely to alter their devices to make a marginal profit. On the other hand, the more aggressively somebody abuses the system, the faster he will be apprehended and appropriately punished.

4 Conclusion and future work

In this paper, we have reported on our ongoing work on the design of mechanisms that stimulate collaboration in both pure ad hoc and multi-hop cellular networks. In particular, we presented two currency-based incentive mechanisms, where nodes that forward packets for the benefit of other nodes are credited and the sources of the packets are charged. In the pure ad hoc case, we protect the proposed mechanism from abuse by implementing some part of it in a tamper resistant hardware module. In the multi-hop cellular case, we rely on auditing performed by the backbone network operator for detecting and punishing abuse of the proposed scheme.

In terms of future work, we intend to explore the way to generalize the proposed incentive mechanisms to other functions than packet forwarding. A further, more general ambition of our research is to explore how mechanisms like the one proposed in this paper could be used for application-level issues. An example thereof could be the mutual provision of information services in ad hoc networks.

In the context of multi-hop cellular networks, we are working on a formal model in which the security properties of our proposed micro-payment scheme can be precisely stated and proven. We are also working on incentive mechanisms adapted for the symmetric case of multi-hop cellular networks.

References

[1] S. Buchegger, J.-Y. Le Boudec, Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes: Fairness in Dynamic Ad-hoc NeTworks), In *Proceedings of the Third ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, Lausanne, June 2002.

[2] L. Buttyán, J. P. Hubaux, Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks, *ACM/Kluwer Journal on Mobile Networks and Applications (MONET)*, to appear, October 2003.

[3] M. Jakobsson, J.-P. Hubaux, L. Buttyán, A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks, In *Proceedings of the Seventh International Financial Cryptography Conference*, Guadeloupe, January 2003.

[4] Y.-D. Lin, Y.-C. Hsu, Multihop Cellular: A New Architecture for Wireless Communications, In *Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (Infocom)*, Tel Aviv, 2000.

[5] P. Michiardi, R. Molva, CORE: A COllaborative REputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks, Technical Report RR-02-062, Eurecom, December 2001.