CASHnet - Cooperation and Accounting Strategy for Hybrid Networks[⋆]

Attila Weyland and Torsten Braun

University of Bern
Institute of Computer Science and Applied Mathematics
Neubrückstrasse 10, 3012 Bern, Switzerland
weyland@iam.unibe.ch , braun@iam.unibe.ch

1 Introduction

Multi-hop cellular networks (also called hybrid networks) increasingly attract interest in the research community. They appear to be a promising combination of the advantages of two worlds: the dynamics of mobile ad hoc networks (MANETs) and the reliability of wired cellular networks. The MANET concept offers advantages attractive to Internet service providers as well as to users. The network becomes dynamically expandable, the network coverage increases and the usage of available network and energy resources can be optimized. In the context of hybrid networks new possibilities to deal with the weaknesses of MANETs become available. We think that besides the security and routing issues the cooperation among nodes is of great importance. We propose a cooperation and accounting scheme, which takes into account the availability of a reliable network infrastructure and stimulates cooperation by making it a rewarding alternative to selfishness. Recently, few approaches have been taken to address the problem of cooperation among nodes in the context of multi-hop cellular networks.

The Nuglets [1] approach enforces cooperation by making the allowance to transmit self-generated packets dependent on the number of forwarded packets. The CONFIDANT [2] approach monitors the behavior of nodes and punishes selfish nodes by means of isolation from the network. The Sprite [3] scheme introduces rewards as incentive for cooperation in MANETs, where nodes report their forwarding activities to a central authority reachable via an overlay network. In [4] the authors suggest the usage of rewards in multi-hop cellular networks and - similar to the approach before [3] - let a central authority collect and analyze reports to decide about rewards and punishments. The authors of [5] and [6] propose similar charging schemes, where cooperative nodes get rewarded in a multi-hop cellular network environment. They both heavily rely on centralized accounting and security mechanisms. In a recent contribution [7] the authors propose a scheme to support both MANETs and multi-hop cellular networks.

With our scheme we provide decentralized accounting and security mechanisms to the largest extent possible in a multi-hop cellular network environment. We support initiator- and receiver-based payments and we do not require full route information from the sender to the receiver. Also, our approach coexists with ad hoc only traffic in the sense that nodes get neither charged nor remunerated for this kind of traffic. We think that ad hoc only communication should be free since the provider has no cost in terms of network traffic. Because we target multi-hop cellular networks in civilian use, where each node can be seen as its own authority, we leave the choice of cooperation to the node. But by providing monetary rewards we make cooperation among nodes a gainful alternative to selfishness.

2 CASHnet Architecture

In our scheme called CASHnet, we assume - similar to the Nuglet approach - the existence of a tamper resistant device, such as a smart card in each node. This device ensures a protected environment, where our schemes' functions can be executed safely. Also, we assume the availability of a routing algorithm, which provides the hop count to the base station (e.g. AODV or DSR). Additionally, we require sufficient amount of processing power and memory on the node.

Our charging/rewarding mechanism works as follows: Every time a node wants to transmit a self-generated packet, it has to pay with *Traffic Credits*. Every time a node forwards a packet it gets *Helper Credits*. Traffic Credits can be obtained from gateways, Helper Credits can be traded in at gateways

[⋆] The work was supported by the Swiss National Science Foundation through the MIPTel project under grant 20-68086.02.

for Traffic Credits. Gateways provide the interconnection between the fixed networks and the multi-hop cellular networks. On one hand, the possibility to obtain Traffic Credits from a centralized source (e.g. a provider) at any time prevents starvation of a node and on the other hand the possibility to earn Helper Credits stimulates the cooperation among nodes. When a customer decides to exchange her Helper Credits for Traffic Credits she has to do that on the provider's location. One could think of a service station, which transforms the Helper Credits according to the customers wish (e.g. Traffic Credits or other offers). This resembles closely to a prepaid service, where a customer "loads" her card at the providers shop. The abstract unit of *Credits* is used as virtual currency which can be replaced by any real currency. The maintenance of two accounts combined with the controlled exchange of Helper Credits makes fraud and misuse difficult.

Our security mechanisms are based on public key cryptography. First, a customer subscribes with her provider, where she gets her personal smart card, which maintains two accounts, one for Traffic and one for Helper Credits. It also contains a public/private key pair, a public key certificate as well as the provider's public key. The public key certificate consists of a unique identifier of the smart card system, the given public key as well as a digital signature by the provider (acting as the certificate authority). To reduce computational costs, each node keeps a list of its next-hop neighbors' identities and their corresponding public key after their successful verification using the operator's public key stored on the smart card. A node also includes in the list the identity and the public key of each successfully verified originator of packets forwarded by the node. To authenticate a node, its public key is required. Therefore, the public key also needs to be sent along with the first initialization packet. This packet also gives feedback if there is a route with cooperative nodes available.

Each self-generated packet is signed before transmission. Each forwarding node verifies the packet upon reception. A forwarding node (except the first one along the path to the gateway) has to verify two signatures, first the one on the packet from the previous hop and then the one on the encapsulated original packet. This ensures non-repudiation meaning that nodes cannot deny having sent the packets. Non-repudiation provides automatically data integrity and data origin authentication. Also, each node keeps a list of the signatures from packets it forwarded with the identity of the corresponding next hop. Additionally, a node keeps track of its next-hop neighbors' willingness to cooperate, which is advertised by them. It is important to avoid creating bogus nodes. We enforce that by issuing certificates with short lifetime. The node owner must also return regularly to the provider's service station, to obtain (purchase/exchange) new Traffic Credits.

3 Conclusion

We proposed a highly decentralized accounting and security architecture which provides a solid foundation for a cooperation scheme based on rewards and which is applicable to multi-hop cellular networks. In contrast to previous work we allow selfish nodes, but encourage them to participate in packet forwarding via rewards. Additionally, we allow initiator as well as receiver based payment which - to the best of our knowledge - is not possible in the available schemes. Last, we do not charge nor reward for traffic within the same multi-hop cellular network (ad hoc only traffic), while other schemes do not allow that. Future work will include the simulation of our scheme, the study of possible extensions (e.g. charging for ad hoc only traffic) as well as the specification of the charging and remuneration relation.

References

1. L. Buttyán and J.-P. Hubaux. Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks. *ACM Mobile Networks & Applications*, 8(5), October 2003.
2. S. Buchegger and J.-Y. L. Boudec. Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks). In *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*. Lausanne, Switzerland, June 2002.
3. S. Zhong, J. Chen, and Y. R. Yang. Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks. In *Proceedings of IEEE INFOCOM*. San Francisco, CA, USA, March-April 2003.
4. M. Jakobsson, J.-P. Hubaux, and L. Buttyán. A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks. In *Proceedings of International Financial Cryptography Conference*. Gosier, Guadeloupe, January 2003.
5. N. B. Salem, L. Buttyán, J.-P. Hubaux, and M. Jakobsson. A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks. In *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*. Annapolis, MD, USA, June 2003.
6. B. Lamparter, K. Paul, and D. Westhoff. Charging support for ad hoc stub networks. *Elsevier Journal of Computer Communications*, 26(13):1504–1514, August 2003.
7. N. B. Salem, L. Buttyán, J.-P. Hubaux, and M. Jakobsson. Stimulating Cooperation in Ad Hoc and Multi-hop Cellular Networks. Poster Session of MICS Scientific Conference, October 2003.