Cooperation and Accounting Strategy for Multi-hop Cellular Networks

Attila Weyland Torsten Braun

{weyland|braun}@iam.unibe.ch

Institute of Computer Science and Applied Mathematics
University of Bern
Neubrückstrasse 10, 3012 Bern, Switzerland

1 Introduction

Multi-hop cellular networks (also called hybrid networks) appear to be a promising combination of the dynamics of mobile ad hoc networks and the reliability of infrastructured wireless networks. These hybrid networks offer several advantages for users as well as operators. The network topology can be dynamically adapted to the respective needs reducing installation costs for the provider, the overall coverage area can be extended and nodes can reduce their energy consumption for transmitting packets due to shorter distances. However, several weaknesses known from mobile ad hoc networks persist. In the context of hybrid networks new possibilities to deal with these weaknesses become available. Besides the security and routing issues the cooperation among nodes is of great importance.

We propose a cooperation and accounting strategy for hybrid networks called CASHnet, which stimulates cooperation among nodes by making it a rewarding alternative to selfishness. Our scheme incorporates a security architecture, which is based on public key cryptography and uses digital signatures and certificates.

Several proposals have been made to stimulate cooperation among nodes. The first approaches were aimed at mobile ad hoc networks and enforced cooperation by threat of punishment. In the Nuglet [1] scheme a node can only transmit self-generated packets when it has forwarded enough packets from its neighbors before. In the CONFIDANT [2] approach the behavior of a node is monitored by its neighbors and a selfish node will be isolated from the network. In both concepts a node can be excluded from participating in the network without itself being at fault (starvation or collective false accusation).

With the Sprite [3] scheme rewards have been introduced as incentive for cooperation in mobile ad hoc networks. Nodes report their forwarding activities to a central authority reachable via an overlay network. In conjunction with the missing security mechanisms this scheme seems highly vulnerable to attacks and transmission errors. In [4] the authors suggest the usage of rewards in multi-hop cellular networks and let a central authority collect and analyze reports to decide about rewards and punishments. However, the authors assume a single-hop down-link (from the base station to the node), which might not be available easily.

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. To remunerate intermediate forwarding nodes, both schemes require the complete route information from the sender to the receiver (e.g. using source routing). However, source routing does not scale well under high node mobility. Also, both schemes do not support cost sharing between sender and receiver, when both of them reside in different

ad hoc networks. The sender also has to pay for the distance from the gateway to the destination. To better cope with misuse the authors of [5] require all the network traffic to go via the operator's access points, which leads to inefficient routes for traffic within the same ad hoc network. [6] requires an existing AAA infrastructure, which might not be available for all multi-hop cellular network scenarios. In a recent proposal [7], the authors extended their work from [5]. They introduced a local Nuglet counter for each node to address the issues of inefficient routes in pure mobile ad hoc networks and a central auditing entity [4] to better cope with abuse. The weaknesses of the Nuglet scheme, such as the unresolvable starvation of selfish nodes due to a single counter and the unsuitability for civilian (commercial) applications because of neglecting the node's freedom of choice (to cooperate or to not cooperate) remain as well as the single-hop down-link.

2 Architecture and Operation

In our scheme we assume - similar to the Nuglet [1] approach - the existence of a tamper resistant device, such as a smart card in each node. This device ensures a protected environment, where the functions of our schemes 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 processing power and memory on the node.

For our scheme we define an architecture as displayed in Figure 1. The CASHnet charging and rewarding mechanism works as follows: Every time a node wants to transmit a self-generated packet (i.e. node O), it has to pay with *Traffic Credits*. Every time a node forwards a packet (i.e. nodes N_{A1} - N_{A3} and N_{B1}), it gets *Helper Credits*. Traffic Credits can be bought for real money or traded for Helper Credits at service stations. Gateways provide the interconnection between the fixed networks and the mobile ad hoc networks.

Our security mechanisms are based on public key cryptography. Nodes authenticate themselves using certificates issued by the provider. To avoid the creation of bogus nodes, we give a short lifetime to the certificates to ensure that the node owner regularly visits a provider's service station. Transmitted messages are digitally signed to provide non-repudiation (data integrity and data origin authentication).

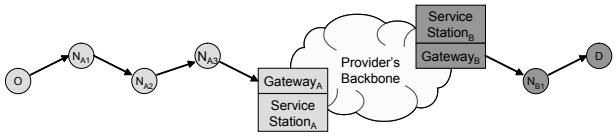

Figure 1: Example Scenario

The operation of CASHnet is described in the following paragraphs. Figure 1 shows an example scenario to which all the defined steps can be applied. The following notation is used: each paragraph describes a coherent phase of the operation process. A phase consists of several enumerated actions, which are executed consecutively. The processing of a phase can be terminated by a reference to another phase "⇒" or by a termination command "□". Numbered list entries in the form of questions indicated a forking of the processing path. Either the "[Yes]" or the "[No]" path is executed. The nested numbered elements of the chosen path are again executed consecutively.

Setup Phase Before a node N can participate in the hybrid network belonging to operator P, node N has to perform the following steps:

1. Obtain a personal smart card from provider P which contains node N's unique identifier, node N's public/private key pair K_N/KP_N, a certificate $Cert_P(ID_N, K_N)$ issued by the provider, as well as the provider's public key K_P (one-time action).
2. Update node N's certificate $Cert_P(ID_N, K_N)$ (as necessary).
3. Load the Traffic Credits account at the provider's service station by paying with real money and/or by transferring Helper Credits (as necessary).

Initial Authentication Phase Before a node can engage in the communication as a packet originator O in the hybrid network, it has to initially authenticate

itself once to all nodes participating in its communication (intermediate nodes N and destination node D). This is done by sending an AUTH Request message to the destination. This message contains O's identifier ID_O, its public key K_O and the certificate $Cert_P(ID_O, K_O)$. Each node N along the path verifies the certificate $Cert_P(ID_O, K_O)$ and - if valid - saves O's identity ID_O and public key K_O as a pair in an AUTH list. After the successful validation of an AUTH Request message, the destination sends back an AUTH Reply message to the originating node O. When node O receives the AUTH reply message, it knows that a path with cooperative node exists and can start with the transmission of self-generated data packets.

Also, every intermediate node N participating in the communication needs to authenticate itself to the previous and the next node along the path. To reduce the delay caused by unauthenticated nodes on a forwarding path, each node in the hybrid network authenticates itself to all it's one-hop neighbors. The identity and public key pairs of successfully authenticated neighboring nodes are also stored in the AUTH list.

If a route changes and a new node joins the path, it is already authenticated to its one-hop neighbors due to the periodic neighboring authentication, yet the new node has to authenticate the originator of the packet, which might cause a small delay.

Packet Generation Phase When a node O wants to transmit a self-generated data packet to the destination D, node O performs the following steps:

1. Is the packet going to leave node O's ad hoc network via the gateway?

   No. (a) The packet classifies as ad hoc only traffic and therefore O does not get charged.
   (b) Form a signed packet $Packet_O$ and transmit it to the next cooperative hop. □

   Yes. (a) Determine the transmission cost of the packet. (The transmission costs are related to the distance in hop counts to the gateway of O's ad hoc network.)
   (b) Does O's Traffic Credits account allow to pay for the transmission cost?

   No. O can not transmit a self-generated packet at this time. □

   Yes.i. Debit O's Traffic Credits account according to the transmission cost (sender-based payment).
   ii. Form a signed packet $Packet_O$ and transmit it to the next cooperative hop. □

$$Packet_O = ID_O|Payload|Timestamp_O| \\ Sig_O(Payload, Timestamp_O)$$

Packet Reception Phase When a node N receives a data packet $Packet_{N-1}$, it performs the following steps:

1. Does the digital signature from the received data packet Sig_{N-1} as well as from the encapsulated original packet Sig_O verify correctly?

   No. Discard the packet. □

   Yes. Proceed to the next check.

2. Does the packet originate from outside node N's ad hoc network and has the destination D been reached (node N equal node D)?

   No. Proceed to the next check.

   Yes. (a) Determine the reception cost of the packet. (The reception costs are related to the distance in hop counts to the gateway of D's ad hoc network.)
   (b) Debit D's Traffic Credits account according to the reception cost (receiver-based payment).
   (c) Form a signed ACK message ACK_N and send it to node $N-1$.
   (d) Pass packet to the non-secured part of node N. □

3. Does the packet originate from within node N's ad hoc network and is it not going to leave node N's ad hoc network via the gateway?

   No. Proceed to the next check.

   Yes. Proceed to the Packet Forwarding Phase (no accounting for ad hoc only traffic). ⇒

4. Does the packet originate from the previous node $N-1$?

No. (a) Form a signed ACK message ACK_N and send it to node $N-1$.

(b) Proceed to the Packet Forwarding Phase. $\Rightarrow$

Yes. Proceed to the Packet Forwarding Phase (no reward for the packet originator). $\Rightarrow$

$$ACK_N = ID_N|Timestamp_N| \\ Sig_N(Sig_{N-1}, Timestamp_N)$$

Packet Forwarding Phase When a node N transmits a forwarded data packet, it performs the following steps:

1. Discard the information from the previous node $N-1$ to retrieve the encapsulated original packet $Packet_O$.
2. Form a signed packet $Packet_N$.
3. Look up the next hop in the routing table towards the destination D.
4. Save the next hop identity ID_{N+1} and the signature of the packet to be forwarded Sig_N as a pair in a list.
5. Transmit the packet $Packet_N$ to the next hop.

$$Packet_N = ID_N|Packet_O|Timestamp_N| \\ Sig_N(Packet_O, Timestamp_N)$$

Rewarding Phase When a node N receives an ACK message from a successor node $N+1$, node N performs the following steps:

1. Does the digital signature from the received ACK message Sig_{N+1} verify correctly?

   No. Discard the message. $\square$

   Yes. Proceed to the next check.

2. Do the contained digital signature of the acknowledged packet Sig_N and the successor node's identity ID_{N+1} have a matching pair in the list?

   No. $\square$

   Yes. (a) Credit N's Helper Credits account.

   (b) Remove the matching pair from the list. $\square$

Gateway-specific Extensions The gateway is responsible for forwarding traffic to the fixed network as well as to the ad hoc network. In the first case (ad hoc $\rightarrow$ fixed) it follows the steps of the Packet Reception Phase. The Packet Forwarding Phase however is done differently. The original packet $Paket_O$ is not signed, but sent unaltered towards the destination. The destination might be located in another ad hoc network, so that the packet will have to pass the corresponding gateway of that other ad hoc network. This is the second case (fixed $\rightarrow$ ad hoc). Here the Packet Reception Phase differs from the steps described above. No verification of the packet or transmission of ACK packets is necessary. The Packet Forwarding Phase is executed as described above.

Our architecture allows a gateway to act as a forwarding node for ad hoc only traffic. In this case it follows the steps described in both - the Packet Reception as well as in the Packet Forwarding Phase. As ad hoc only traffic is not remunerated, the Rewarding Phase is not executed.

3 Evaluation

The CASHnet scheme provides incentives for cooperation through monetary rewards. Instead of monitoring and punishing selfish nodes or putting the ability to transmit self-generated packets under the condition of having forwarded enough packets from other nodes, we make cooperation attractive. With the maintenance of separate accounts for traffic generation costs and rewards, we allow selfish nodes in our scheme. A node never has to be cooperative to earn its right for transmission, all it needs is enough Traffic Credits, which can be purchased at the service stations. If the node decides to be cooperative it also can trade in the earned Helper Credits at the service stations. In addition, the separation of accounts allows the provider to actively control the remuneration process of nodes. This enables the provider to build up and maintain strong relations with his customers.

Introducing money into any kind of system increases the risk of fraud. This is true especially in the case of multi-hop cellular networks where each individual node also acts as a router. Therefore we

must take strong security precautions. The tamper-resistant device allows for secure storage of keys and safe execution of functions. Due to the open environment we decided for a public key based infrastructure, which requires no direct key exchange. The use of digital signatures prevents the unnoticed modification of packets and uniquely identifies the packet originating as well as the packet forwarding node. Thus invalid (e.g. unpaid) packets will not be forwarded and rewards can be distributed safely.

The decentralized design has of course impact on the overall architecture requirements. The current security mechanisms (e.g. double signature verification) are costly in terms of processing power. Yet the environment of multi-hop cellular network enforces that we take the maximum security precautions possible and feasible at the same time.

While our security mechanisms ensure non-repudiation and we assume a tamper resistant device, we do not yet actively handle malicious (i.e. non-rational) behavior of nodes. The most obvious could be the dropping of packets to be forwarded using a filter (e.g. a firewall). To cope with this problem we will study the possibility of introducing charges for the reception of packets similar to a deposit. Such a charge would be a fraction of the reward obtained from forwarding the packet. The node would have an incentive to recover the costs imposed by the reception of a packet and therefore more likely forward the packet to obtain the reward.

Anther issue is the coexistence with ad hoc only traffic, i.e. traffic that does not pass the gateway. In our current approach we do not charge for this kind of traffic. On the one hand, this seems fair towards the users, since they can also engage in ad hoc communication without the provider. On the the other hand, a user might try to reduce the cost of transmission by sending a packet ad hoc to a collaborative node located closer to the gateway and let this node "generate" and transmit it via the gateway. One could argue that this behavior is tolerable in the sense that no rewards have been distributed to the intermediate nodes and therefore no monetary loss occurred. Yet the provider makes available the security infrastructure which is also used in ad hoc only communication. Furthermore, these collaborative nodes could encourage the bypassing of our scheme by acting as a reseller offering a favorable price compared to the provider. This could result in a worst case scenario with a few nodes in the direct neighborhood of the gateway re-offering services to a totally uncontrolled ad hoc network. We identified this as a big issue and investigate possible solutions. An obvious solution is the introduction of charges for ad hoc only traffic.

While we could argue that our tamper resistant device protects us against any kind of attack, we feel that it is more realistic to assume that it does not, and therefore we continue study on other feasible ways to reduce the possibility of misuse and the computational costs for the nodes.

4 Summary and Outlook

We propose 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 and introducing deposit payment for receiving 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.