Light-Weight Charging and Accounting in Mobile Ad-Hoc-Networks

Inna Kofman
University of Düsseldorf
Düsseldorf, Germany

Martin Mauve
University of Düsseldorf
Düsseldorf, Germany

1 Introduction

Mobile ad hoc networks (MANETs) [2] are networks that consist of mobile nodes with limited transmission range. In order to allow communication beyond this range, nodes have to forward data on behalf of other nodes. Since a node that forwards a foreign packet spends its own resources, such as battery power, it needs to have a reason to do so. One approach to provide this motivation is to use a charging and accounting scheme to pay the owner of the device a small amount of money for each forwarded data packet.

Existing approaches to enable charging and accounting in mobile ad-hoc networks focus on guaranteeing a fair behavior of every participant. To this end they employ strong cryptography [3] [6] [8] and/or tamper proof devices [1] [4] [7].

It is our idea to take a different approach at charging and accounting in mobile ad hoc networks. This approach is derived from the way rules are enforced in a modern society: there is no guarantee that each individual will follow the rules. However, if someone breaks the rules and commits a crime, he will run the risk of being caught by the police and punished appropriately. This ensures that the rules are followed without incurring the prohibitively high overhead (and other undesired effects) of continuously controlling the behavior of each individual.

Applying this principle to ad-hoc-networks allows nodes to cheat and effectively steal money from other nodes or use their services without payment. Our reasoning is that nodes will not exploit this ability since they will run the risk of being observed, caught, and punished if they would break the rules. As long as the average loss of being caught is higher than the average gain through the illegal action there is no rational reason to cheat.

It is obvious that the decision of a rational individual node whether or not to cheat will depend on the potential average gain and the potential risk and loss of being caught. In the remainder of this short paper we assume that being caught causes an infinite punishment ("the death penalty") whereas the gain of cheating would be finite. We furthermore assume that all nodes behave rational. As a consequence nodes will not cheat if they run any chance of being caught. The key question that then needs to be examined is: can any illegal behavior be detected with at least a minimal positive probability?

In order to investigate this question we introduce a simple model of ad-hoc-networks in Section Two. In Section Three we investigate common approaches to cheat and show that they do have a positive probability of being detected. Finally, Section Four gives an outlook to future work.

2 Model

There are two kinds of nodes in the system: regular nodes and policemen nodes. As the policemen nodes are mobile agents distributed within the network they hear all traffic of nodes in their transmission range. We assume that the policemen nodes cannot be detected by nodes because they just receive but do not relay traffic. Policemen nodes report all collected data about the observed nodes to a central authority that will check whether cheating has happened. Since the number of policemen nodes is significantly smaller than the number of regular nodes and a continuous control of each node is not required, the network monitoring takes place with relatively small overhead.

Here we present a simple model (similar to one introduced in the [4]) that motivates the cooperation of nodes in the MANET. The general idea is that the sender puts a number of coins into the packet. Every intermediate node takes one coin and forwards the packet to the next hop towards the destination. The model is based on following assumptions:

- Every intermediate node is able to determine the "best" next hop toward the destination (for example, using a position-based routing protocol [5]).
- A coin is a unique unit of electronic cash signed by the central authority.
- A policeman node has knowledge about the node location. Also, it can determine whether the next node, which is selected by the monitored node, is the "best" next hop toward the destination.

Coins are purchased in advanced from the central authority. When a node possesses a sufficient amount of coins and wants to send a message it has to form a packet. Except of the message the sender puts there its identifier and the identifier of the node to whom the packet will be sent. To pay the packet transmission the sender preloads into the packet a set of coins.

Thus, if the sender S wants to transmit a message m to the destination D it estimates a number of hops h that is enough to reach D. S sends a packet that contains m, S, D. Also, it includes coins $(C_1, C_2, C_3, ..., C_h)$ as the number of the estimated hops, which were recently gained by the sender:

$$(m, S, D, C_1, C_2, C_3, ..., C_h)$$

Every intermediate node takes one coin (it is unimportant which of them) and forwards the packet to the next one toward the destination:

$$(m, S, D, C_1, C_2, C_3, ..., C_{h-1})$$

As is evident from the foregoing, no cryptographic calculations are needed to form/modify the packet by the sender/intermediary, correspondingly. Therefore, the packet generation as well as the packet forwarding processes are very light weight. Also, the packet contains only essential data for the effective communication, so, the transmission of extra data is relatively small.

3 Monitoring

As was described before, the network is monitored by special policemen nodes. The main purpose of the policemen nodes is to stimulate nodes to act within the predetermined rules. Nodes know that they may be monitored at any time and run the risk of being punished if an illegal action is detected by a police node.

According to the assumption that nodes are rational, they will only cheat and act illegally as long as the average gain of cheating is bigger than the average loss through being punished. For the moment we (unrealistically) assume that the punishment is infinite while the gain is finite and leave the fine-tuning of the punishment to future work. Given these assumptions a node will never cheat if there is at least a minimal positive chance of being caught. Thus a node will not cheat if an arbitrary constellation of police nodes would be able to reveal it as a cheater. It is very important to realize that there is no requirement whatsoever to investigate all nodes all the time. In fact the network can be almost void of police nodes as long as it is theoretically possible to catch any cheater with a positive probability. In particular this condition is fulfilled if a set of perfectly placed police nodes would be able to reveal the cheater.

Therefore the challenge is to show that for each attempt to cheat a perfectly placed set of police nodes would have a positive chance of detecting this attempt.

We have no formal proof of this property, yet. However all individual attempts to cheat that we investigated do meet this requirement. In the following we present some examples how common attacks could be detected by the policemen nodes:

- Double spending of coins. The sender of a packet uses the same coin in two distinct packets. A policeman node is able to detect this if he observes both transmissions.
- Double spending of coins. A node puts into the self-generated packet a coin that does not belong to him originally. After a policeman node reports collected data, the central authority can discover it after it verifies whether all coins preloaded into the packet were recently purchased by the node.
- Illegal action. An intermediate node takes more than one coin from the packet. A policeman node can notice it when he checks whether the set of incoming coins is identical to the outgoing set (except one coin that was taken by the node).
- Illegal action. An intermediate node forwards the packet to a colluding node (by that prolonging the route artificially). A policeman node can detect it if he considers that the chosen node is not the "best" next hop toward the destination.
- Double coin submission. An intermediate node takes one coin (as is expected) and just copies another one of remaining in the packet, and then submits both coins. The node will be considered as a cheater if a policeman node has observed that the copied coin was taken by another node.

4 Conclusion and Future Work

In this paper we proposed a new approach for the charging and accounting problem in MANETs. The approach provides an incentive for cooperation by means of remuneration. In contrast to the existed approaches, nodes are able to behave dishonestly. Also, they are free of dealing with requirements connected to the security. Instead, it is imposed on special policemen nodes which monitor the network from time to time. As a consequence, mobile nodes could fully concentrate on the packet transmission that allows a light-weight (low-latency) communication.

In the future work we are going to provide a formal proof why it is possible to detect any type of attacks of malicious nodes with a minimal positive probability. For that reason we have also to investigate what is the optimal number of the policemen nodes should be for effective monitoring as well as ways of their distribution in the network. Since the simple model presented in the Section 2 is intended just to illustrate the concept, it will be interesting to consider another kinds of models based on our approach. Like, for example, a model with different levels of punishment, which will stipulate that attacker, in addition to monitoring, could be discovered by narrow inquiry with high probability of success. Or models based on different kinds of routing protocol. Also, an extended model that is able to cope with not only rational but as well as irrational/malicious attacks (that was not considered by the existed works). Different models as well as their overhead will be analyzed by means of the simulation.

References

[1] L. Buttyán and J.-P. Hubaux. Enforcing service availability in mobile ad-hoc WANs. In *MobiHoc 2000*, pages 87–96, 2000.

[2] I. Chlamtac, M. Conti, and J. J. Liu. Mobile ad hoc networking: Imperatives and challenges. *IEEE Networks*, 1(1), 2003.

[3] 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.

[4] L.Buttyán and J.-P. Hubaux. Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks. In *ACM Mobile Networks & Applications, 8(5)*, October 2003.

[5] M. Mauve, J. Widmer, and H. Hartenstein. A Survey on Position-Based Routing in Mobile Ad Hoc Networks. *IEEE Network*, 1(6), Dec, 2001, pp. 30–39.

[6] B. Salem, L. Buttyán, J.-P. Hubaux, and M. Jakobsson. A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks. In *In Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, Annapolis, MD, USA, June 2003.

[7] A. Weyland and T. Braun. Cooperation and Accounting Strategy for Multi-hop Cellular Networks. In *In Proceedings of IEEE Workshop on Local and Metropolitan Area Networks (LANMAN 2004)*, pages 193–198, Mill Valley, CA, USA, August 2004.

[8] S. Zhong, J. Chen, and Y. R. Yang. Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks. In *In Proceedings of IEEE INFOCO*, San Francisco, CA, USA, March-April 2003.