

Managing credits in mobile ad hoc networks*

Fabio Martinelli, Marinella Petrocchi, and Anna Vaccarelli

IIT - CNR. Pisa, Italy

{fabio.martinelli, marinella.petrocchi, anna.vaccarelli}@iit.cnr.it

Key words: Mobile Ad Hoc Networks, Selfishness.

Unlike traditional mobile networks, ad hoc networks do not rely on any wired infrastructure. Instead, the network is kept connected by the mobile hosts. In order to make a mobile network functional, the nodes need to be self-organized, in such a way that a message is delivered from a source to a destination through a set of intermediate nodes. The deployment of ad hoc networks for civilian applications is taking a footing. In such applications, the nodes are not governed by a single authority and need not share a common goal (the contrary could be the case in emergency and military applications). Thus, cooperative behaviours, such as forwarding each other's packets, cannot be easily assumed. The single nodes could prefer to save battery life for their own communication, rather than to forward packets for other nodes. Such an attitude is denoted in the recent literature as *selfishness* of the node. Simulation results (see, *e.g.*, [7]) have recently pointed out that a selfish behaviour can be as harmful, in terms of the network throughput, as a malicious one.

There is a growing interest in the research community for detecting and preventing a selfish behaviour, and promoting cooperation between nodes, (see, *e.g.*, [1, 2, 5, 6, 8, 10]). Our research deals with the matter by proposing an infrastructure for a local management of credits (*i.e.*, a measure of how many packets node A has forwarded to node B, from A's point of view), and debits (*i.e.*, the same measure, but now from B's point of view). Each node maintains this information in a local repository that we call *credit table*, on which the node can rely to judge the past behaviour of the other nodes in the network. More specifically, we define precise rules for the table initialization, its maintenance, and secure acknowledgments testifying the actual forwarding of packets in the network. Data recorded in the table does not propagate over the network and they are obtained through trusted second-hand information. We equip the network under investigation with a secure infrastructure, in order to provide authentication and integrity to the second-hand information.

We particularly focus our attention on bootstrapping trust within our architecture. Hosts in mobile networks are indeed prone to the following security threat: if i) users are punished for their selfish behaviour, or ii) new users entering the network are *a priori* granted to have an initial amount of packets forwarded, then a node could be tempted to discard its initial identity and re-enter the network in disguise. Hence, we propose a solution providing strong authentication

* Submitted to 2nd UK-UbiNet Workshop – Trust in ad-hoc collaborations session.
Contact author: marinella.petrocchi@iit.cnr.it

of the user, in order to achieve a univocal relation between a physical device and the identity it claims at its first steps in the network. Briefly, the central idea is that, by virtue of the media over which data are sent, a credential can be achieved by an authority in a non forgeable way, and univocally identifies a device for its activities in the network. Our trust setup is based on some transmission features of so called *Location Limited Channels*, out of band communication media originally introduced by [9]. The latter use LLCs for pre-authentication between devices that successively communicate with each other. We suggest an extension of the use of LLCs, in order to assigne unique credentials to mobile devices, thus avoiding a return to the network in disguise.

Some authors assume a selfish node may have also an active behaviour, located somewhere between a non-cooperative behaviour and a misbehaviour aiming at damaging the others. Then, we assume the following: a selfish node could not cooperate to the basic network functioning (such as packet forwarding) and it could also illegally act in order to obtain benefits for sending its own packets (*e.g.*, by maliciously increasing its level of reputation). Hence, if an adversary adds virtual nodes to a route which it belongs to, then it could lead the adversary to gain awards, if that route behaves well in terms of packet forwarding (it is assumed that the adversary *owns* those added virtual nodes, and it consequently takes the credit for the correct behaviour of these nodes). Thus, at routing level we assume Ariadne [3] the secure version of the on-demand protocol DSR [4] providing authenticity of routing packets.

We propose to use network-layer acknowledgments (additional data in routing protocols specifications like [4]) to provide to the packet source an authenticated proof that its packet has been delivered to destination. We specify a precise structure for the acknowledgment request and the corresponding acknowledgment. Then we introduce the concept of *block acknowledgment*, *i.e.*, a mechanism that amortizes the signaling of “occurred delivery” over blocks of n data packets, thus reducing the communication overhead on the way back from destination to source. Further, we deal with some kind of attacks to which our scenario is prone. As an example, we consider free riding attacks, where an intermediate node of a route may append (or substitute) its own payloads to the data packets transmitted from the source to the destination. To avoid that other nodes in the route charge the source, we provide authentication of origin and integrity to the data packets, by exploiting a hash chain-based technique. The security features are applied to the whole packets, thus securing both the data and the packet header (and consequently the acknowledgment requests).

Finally, in the model we have developed, if node A behaves well in forwarding packets to node B, then it can exploit this correct behaviour only with B (meaning that A may rely on routes including B for sending its packets). Intuitively, systems based on such a rule can get stuck. Then we introduce the notion of credits *transferring*, according to which A may ask B to transfer, in a secure way, its credits to some other nodes.

We remark that the proposed architecture must be supported by simulations in order to evaluate its impact on the network throughput.

References

- [1] S. Buchegger and J. L. Boudec. Performance Analysis of the CONFIDANT Protocol. Cooperation Of Nodes - Fairness In Dynamic Ad-hoc Networks. In *Proc. of ACM MobiHoc'02*, 2002.
- [2] L. Buttyan and J. Hubaux. Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks. *ACM/Kluwer Mobile Networks and Applications (MONET)*, 8(5), 2002.
- [3] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In *Proceedings of the Eighth ACM International Conference on Mobile Computing and Networking (Mobicom 2002)*, 2002.
- [4] D. Johnson, D. Maltz, and J. Broch. DSR The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks. *Ad Hoc Networking, chapter 5*, pages 139–172, Addison-Wesley, 2001.
- [5] S. Marti, T. Giuli, K. Lai, and M. Baker. Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks. In *Proc. of MobiCom'00*, pages 255–265. ACM, 2000.
- [6] P. Michiardi and R. Molva. Core: a collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks. In *Proc. of CMS'02*, 2002.
- [7] P. Michiardi and R. Molva. Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks. In *Proc. of European Wireless'02*, 2002.
- [8] N. B. Salem, L. Buttyan, J. Hubaux, and M. Jakobsson. A charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks. In *Proc. of ACM MobiHoc'03*, 2003.
- [9] F. Stajano and R. Anderson. The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks. In *Proc. of 7th Security Protocols Workshop*, volume LNCS 1796, pages 172–194, 1999.
- [10] S. Zhong, J. Chen, and Y. Yang. Sprite: a Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks. In *Proc. of IEEE Infocom'03*, 2003.