Abstract—This paper presents an analysis of MAC layer misbehaviour in 802.11 mobile ad-hoc networks. Such misbehaviour can be performed, e.g., to achieve greater throughput or extended battery life. Focus is put on actions which are both easy to perform and give substantial benefits to the misbehaving node. In particular, the new IEEE 802.11e standard, which defines QoS enhancements, is taken into account. This standard has introduced significant changes in the MAC layer of WLANs which can potentially be exploited. This paper provides a state-of-the-art look at possible vulnerabilities in the MAC layer and an analysis of their usefulness to malicious users. It also presents preliminary simulation results from ongoing research.

Index Terms—Ad-hoc networks, misbehaviour, QoS, simulations.

I. INTRODUCTION

Mobile ad-hoc networks (MANETs) rely on node cooperation to ensure communication and to efficiently achieve user goals. All currently used protocols were designed with the assumption that every participant follows the rules. However, there is a severe security threat in misbehaviour – when nodes stop cooperating in order to increase their own gains (such as higher throughput or extended battery life). The detection and mitigation of such actions plays an important role in order to provide QoS in MANETs.

The 802.11 MAC layer was designed to share the wireless channel in a cooperative way. The distributed contention mechanism (CSMA/CA) of 802.11 assumes that all nodes behave properly. However, nodes may obtain an unfair throughput share from not obeying the MAC mechanism. Such benefits can be obtained by selecting a smaller backoff, not doubling the contention window (CW), changing default inter-frame times, manipulating NAV, etc. MAC layer misbehaviour can lead to more significant bandwidth gains than misbehaviour at the network and transport layers. At the same time it is hidden from detection mechanisms working in the higher layers.

This paper presents a work-in-progress which deals with the important and unresolved problem of node misbehaviour. It aims to answer the following questions: What type of misbehaviour is the easiest and most beneficial to perform? What is the impact of misbehaviour on QoS provisioning?

The rest of the paper is organized as follows. Section II provides state-of-the-art in detecting and providing countermeasures for MAC layer misbehaviour. The impact of 802.11e on misbehaviour is discussed in Section III. Preliminary simulations are shown in Section IV. Section V concludes the paper and describes future work.

II. STATE OF THE ART

The problem of MAC layer misbehaviour has been the subject of recent studies. The authors of [5] propose a solution to the problem of nodes choosing smaller backoff values. In their approach, the receiver decides on the value and provides it to the sender by CTS and/or ACK frames. This was designed with infrastructure WLANs in mind where it was assumed that the AP was well-behaved. An extension for ad-hoc networks, where the receiver can be tested for misbehaviour, is also analyzed. However, the main drawback of this solution is that it requires changes to the 802.11 standard.

DOMINO, the solution described in [6], does not require any such changes. It was designed to ensure fairness in hot-spot scenarios and takes into account both selfish and malicious actions (e.g., jamming). Even though the applied detection mechanisms are advanced, such a solution could not be used in ad-hoc networks because they lack a central point of authority.

The authors of [2] deal with backoff misbehaviour in MANETs. They propose a distributed random backoff value selection method to thwart node selfishness. A reputation scheme similar to the one presented in [1] is used to identify misbehaving nodes.

III. MISBEHAVIOUR IN 802.11E

The IEEE standard for ensuring QoS in WLANs (802.11e [4]) was also designed with the assumption that all nodes behave properly. However, it introduces new opportunities for misbehaviour in the MAC layer. Such parameters as AIFS, CWmin, CWmax, and TXOP have become easy to alter. The influence of this kind of misbehaviour has not yet been thoroughly studied and there are many open questions. Can a misbehaving node manipulate the aforementioned parameters...
to achieve better throughput in both uplink and downlink
directions? Would this gain be irrespective of traffic type
(TCP/UDP)? Can such a node decrease the throughput of
other nodes in the MANET by assigning lower priorities to
to their traffic? These questions are the subject of study in this
work-in-progress.

IV. PRELIMINARY SIMULATIONS

To determine the impact of MAC layer misbehaviour on
802.11e-based ad-hoc networks, preliminary simulations have
been performed. They were done using the ns-2 simulator with
the TKN implementation of the EDCA model [7]. A small
802.11b (11 Mb/s) network of 5 nodes was considered, as
shown in Figure 1.

![Simulation topology](image1)

Figure 1. Simulation topology

All stations were within hearing range of each other. They
were sending CBR traffic (DATA-ACK exchange). The frame
length was set to 1000 bytes. In order to test the impact of
choosing smaller CWmin and CWmax parameters the priority
of the traffic was set to _background_ (CWmin = 31, CWmax =
1023). One of the nodes (the ‘bad’ node, encircled)
misbehaved by setting these parameters to (CWmin = 1,
CWmax = 5). The results of these preliminary simulations can
be seen in Figure 2 (Figure 3) for node throughput (packet
delay) as a function of the CBR rate.

![Throughput vs. CBR rate](image2)

Figure 2. Throughput vs. CBR rate

![Packet delay vs. CBR rate](image3)

Figure 3. Packet delay vs. CBR rate

V. CONCLUSIONS AND FUTURE WORK

The preliminary simulations have shown that a misbehaving
node can expect to dominate network utilization. The packet
delay is lowered significantly and the gain in throughput is
limited only by the channel capacity. Further simulations are
required to determine the effects of changing other 802.11e
parameters. More complex network scenarios will be
considered, with more realistic traffic patterns. The result of
this study will be determining what are the most likely forms
of misbehaviour in the MAC layer – both easy to perform and
giving significant advantages to the users. Future work will
also involve studying detection mechanisms for given
misbehaviour types, as well as the impact of similar actions on
other layers (results concerning IP layer misbehaviour have
been shown in [3]).

REFERENCES

Prevention of MAC Layer Misbehavior for Ad Hoc Networks”,
and Misbehavior – A File Sharing Case”, First Workshop on Operator-
assisted (Wireless Mesh) Community Networks, 18-19 September 2006,
Berlin, Germany.
Telecommunications and information exchange between systems—
Local and metropolitan area networks—Specific requirements Part 11:
Wireless LAN Medium Access Control (MAC) and Physical Layer
(PHY) specifications; Amendment 8: Medium Access Control (MAC)
Quality of Service Enhancements.
Wireless networks”, IEEE Transactions on Mobile Computing, Volume
4, Number 5, September/October 2005.
Layer Greedy Behavior in IEEE 802.11 Hotspots”, IEEE Transactions
Model for ns-2”, Technical Report TKN-06-003, Telecommunication
Networks Group, Technische Universität Berlin, June 2006.