Paper

Application of a hash function to discourage MAC-layer misbehaviour in wireless LANs

Jerzy Konorski and Maciej Kurant

Abstract—Contention-based MAC protocols for wireless ad hoc LANs rely on random deferment of packet transmissions to avoid collisions. By selfishly modifying the probabilities of deferments greedy stations can grab more bandwidth than regular stations that apply standard-prescribed probabilities. To discourage such misbehaviour we propose a protocol called RT-hash whereby the winner of a contention is determined using a public hash function of the channel feedback. RT-hash is effective in a full hearability topology, assuming that improper timing of control frames is detectable and that greedy stations do not resort to malicious actions. Simulation experiments show that RT-hash protects regular stations' bandwidth share against various sophisticated greedy strategies of deferment selection; as such it may contribute to MAC-layer network security.

Keywords—wireless LAN, MAC protocol, noncooperative setting.

1. Introduction

Ad hoc wireless packet networks offer the possibility of cheap on-demand interconnection of a set of stations (mobile user terminals) in an environment where any fixed communication infrastructure would turn out either physically or economically infeasible [1]. As the underlying technology matures, ad hoc networks expand from their traditional niche of disaster management and military systems to public local- and wide-area data communications and become an attractive alternative to costly wireline networks. This expansion, however, brings new design challenges that are critical to ad hoc networks' long-term survival. Namely, adherence to the deployed standard communication protocols can no longer be counted on for several reasons. Firstly, if the stations of an ad hoc network are not subjected to a common authority then there are no administrative facilities like log-in, traffic monitoring, service accessibility, conformance testing etc., which implies that punishment for a station's misbehaviour can only be enforced by other stations in a distributed fashion. Secondly, ad hoc networks guarantee a certain degree of anonymity—any station may disappear at any time (switch off, move out of range or switch identity) and reappear later pretending to be another station; therefore it need not fear any punishment that does not materialise instantly. For example, ill reputation based on cumulative statistics of past packet transmissions [2] would not make a serious disincentive to stations willing to misbehave. The emergent noncooperative design paradigm is now establishing itself as a part of wireless network security planning [3].

In this paper we focus on MAC-layer selfish misbehaviour whereby a station may depart from the standard rules of contention for the wireless channel so as to grab a larger-than-fair share of the available bandwidth. Such misbehaviour is indeed possible, contrary to the popular opinion that adherence to standard MAC protocols is only natural if the stations want to stay "synchronised" [4]. Consider the class of distributed MAC contention protocols, sometimes referred to as random token (RT) [5], that rely on random deferment of packet transmissions for collision avoidance. These include HIPERLAN/1 [6] and CSMA/CA with RTS/CTS exchange [7], later incorporated into the IEEE 802.11 MAC standard [8]. In any instance of contention the winner is the station whose deferment is extreme among the contending stations; this condition is equivalent of capturing a unique token that visits the stations in random order rather than sequentially. By manipulating the probability distribution of transmission deferment a station can easily outperform stations that apply a standard-prescribed probability distribution [9, 10].

The purpose of this paper is to propose a new protocol called RT-hash in order to prevent MAC-layer misbehaviour. Specifically, we propose to determine the winner of a contention using a public hash function of the feedback each station gets from the contention. This is hoped to confuse misbehaving stations in such a way that no modification of the probability distribution of transmission deferment should appear beneficial to them. Given that, they may resort to more sophisticated deferment selection strategies, which we attempt to anticipate and the impact of which we attempt to evaluate.

Note that the feedback from a contention is implicitly assumed to be uniform across all stations; this implies a single-hop wireless LAN (WLAN) setting and perfect channel operation. We believe that, although hidden stations and transmission errors may affect the protocol we propose, the illustrative and qualitative value of the presented results will not be diminished.

The paper is organised as follows. In Section 2 the network model and a framework for MAC-layer misbehaviour are outlined. Section 3 presents the RT-hash protocol against the background of earlier RT-like protocols and examines the requirements for the public hash function, assuming random selection of transmission deferments. In Section 4

some sophisticated selection strategies are discussed; their impact on the RT-hash protocol is evaluated in Section 5. Section 6 concludes the paper.

2. The model

We consider a number of stations interconnected by a single-channel wireless network. The proposed model reflects the general idea of an ad hoc system outlined in Section 1. We begin with the network station model and then present our model of MAC-layer misbehaviour.

2.1. The network station model

As can be expected of an ad hoc system, the station model mostly consists of non-assumptions. Namely we accept that a station need not:

- stay interconnected all the time or maintain a permanent identity; thus in general the number of stations N need not be fixed or known,
- communicate its present identity to any station other than the recipient(s) of its current transmission; thus from the viewpoint of the MAC protocol the stations are anonymous,
- interpret any transmitted data of which it is not an intended uni- or multicast recipient (except for detecting carrier on the channel); thus it can fully encrypt its communications and use any data format it has agreed on along with the current recipient(s).

To remove the dependence on a particular hearability topology, station mobility model, multihop packet forwarding protocol and traffic scenario, as well as the physical characteristics of the wireless channel, we also assume that

- all stations hear each other's transmissions directly, i.e., the network is a single-hop WLAN,
- each station always has a packet ready to send, i.e., the network operates under heavy load conditions, and
- the characteristics of the wireless channel and the attained signal-to-noise ratio ensure error-free transmission between any pair of stations.

Further, to simplify the presentation of the RT protocols, we assume that each station synchronises to a global slotted time axis. A slot allows for a transmission and reception of a MAC protocol's control frame and leaves enough time for each station to decide the type of the slot based on the feedback from sensing the channel. A station distinguishes v- or c-type slots sensed, for "void" or "carrier"; moreover, a recipient of a successful (i.e., non-colliding) transmission recognises an s-type slot, for "success", and reads its contents. This type of binary feedback facilitates collision avoidance and is employed in deferment-based MAC protocols, e.g., in the form of RTS/CTS exchange [7, 8]. We shall prefer the term *pilot/reaction mechanism* instead of RTS/CTS in reference to a generic RT protocol to stress that the format and semantics of the involved control frames may differ from those specified by the IEEE 802.11 standard.

In the pilot/reaction mechanism each station synchronises to the start of a protocol cycle, marked by a v-type slot following a packet transmission. Subsequent slots are classified by all the stations as *contention slots*, in which pilot frames can be transmitted, and *reaction slots*, reserved for reaction frames. The first slot of a protocol cycle is a contention one; any c- or s-type contention slot is followed by a reaction slot and then another contention slot; a v-type contention slot is followed by another contention slot. A station with a packet ready defers for a number of slots (the *transmission deferment*) and transmits a pilot. Further action depends on the channel feedback the station gets in the following reaction slot. The transmission deferment may vary from one protocol cycle to another as dictated by a *selection strategy*. In existing RT protocols this number is drawn from a uniform probability distribution over a range of values; such a strategy will be called *Randomiser*. It should be noted, however, that the selection strategy need not be a part of the protocol; strictly speaking, the protocol only defines the rules of contention such that all the stations can reach a consensus regarding the winner or a no-winner outcome.

2.2. Model of MAC-layer misbehaviour

A taxonomy of ad hoc station misbehaviour presented in [11] suggests distinguishing selfish and malicious misbehaviour; this roughly corresponds to rational vs. irrational motivation for departures from standard protocols. Selfish MAC-layer misbehaviour is rational in that a station may want to grab a larger-than-fair share of the available bandwidth, but will not act just to reduce other stations' throughput without a clear benefit for its own. For example, issuing unnecessary pilots or jamming other stations' transmissions "for the fun of it" is irrational in terms of own throughput and power consumption. In the context of RT protocol, selfish misbehaviour can be twofold: a station can either violate the rules of contention or adopt a selection strategy other than Randomiser. The former type of misbehaviour would have to involve improper timing of pilot/reaction frames; e.g., a station might transmit several pilots in a protocol cycle while the rules of contention allow only one. Such behaviour is detectable by means of a directional antenna and as such could in principle be immediately punished. On the other hand, tampering with a selection strategy is hard to detect and prove by other stations. Long-term statistical analysis of transmitted packets might reveal significant departures from Randomiser; unfortunately such an approach is pointless in view of the assumed station anonymity and packet encryption.

Following the approach in [9, 10], we wish to develop an RT-type MAC protocol for which no rational selection strategy will perform substantially better than Randomiser. The following framework for MAC-layer misbehaviour is assumed:

- all N stations comply with the rules of contention,
- G stations are *greedy*, i.e., willing to grab a larger-than-fair share of the available bandwidth; these are free to use any selection strategy (G need not be fixed or known to any station),
- the other N–G stations are *regular*, i.e., apply Randomiser,
- a greedy station acts in isolation, i.e., cannot coordinate its selection strategy with other greedy stations.

The last assumption may seem controversial. It is reasonable if one presumes that stations are reluctant to reveal their greedy status to others. However, collusion among some greedy stations is not unthinkable [12]. In fact, a worst-case greedy selection strategy we consider in Section 4.3 approaches a collusion scenario.

3. Random token protocols

The RT-hash protocol presented in this section breaks with the rule requiring that the winner's deferment be extreme among the contending stations. To clarify this difference we first briefly summarise some earlier RT protocols [10].

3.1. RT and RT-1s protocols

A station with a packet ready to send selects a deferment between 0 and D–1 contention slots (D is an integer parameter) and when it expires, transmits a pilot frame. The pilot contains the recipient's identity (possibly in an implicit manner, e.g., using the recipient's public or symmetric encryption key) and in addition may contain the first fragment of the packet. Since full encryption is allowed, to all non-recipients the pilot is merely a burst of non-interpretable carrier. If at some station the frame decrypts to a correct pilot, that station has just sensed an s-type slot and recognised itself as a recipient. In such a case it issues in the following reaction slot a reaction frame that is merely a burst of carrier. Having sensed the reaction slot following the pilot as c-type, the sender of the pilot continues to send the remaining part of the packet. A lack of reaction (i.e., a v-type reaction slot) marks a pilot collision and terminates the protocol cycle (Fig. 1). Note that a greedy station can do no harm by jamming a reaction frame. Nor can it benefit from issuing a reaction frame if it is not a recipient or from not issuing one if it is a recipient.

Under RT, greedy stations need only a minor alteration of the standard random selection strategy to monopolise the channel bandwidth. A modified protocol called RT-1s (for "first success") [10] is somewhat more resistant to greedy stations. Under RT-1s, stations whose pilots were not reacted to back off until the next protocol cycle, while the rest are free to transmit their pilots in subsequent contention slots (Fig. 2). Note that the back-off provision implies that the threat of misbehaviour detection using a directional antenna is serious enough to discourage greedy stations from transmitting more than one pilot per protocol cycle. Also note that the start of a protocol cycle is now marked either by the termination of a packet transmission or by D consecutive v-type slots (in this regard D is an analogue of DIFS in IEEE 802.11).

3.2. RT-hash protocol

Random token-hash aims to improve on RT-1s in the presence of greedy stations. The protocol operation is illustrated in Fig. 3. A station with a packet ready to send defers for a number of contention slots between 0 and D–1. Subsequently it transmits a pilot and awaits a reaction. Now each intended recipient transmits a reaction if an s-type slot is sensed, while refraining from reaction if a c-type slot is sensed. The presence or absence of a reaction permits the other stations to deduce that the previous slot was s- or c-type, respectively.

When D contention slots have elapsed, along with the corresponding reaction slots (if any), all stations arrive at an identical *feedback vector* $\mathbf{f} = (f_1 \dots f_D)$ with $f_i = 0, 1$ or 2 if the ith contention slot was v-, s- or c-type, respectively. Denote $S(\mathbf{f}) = \{i \,|\, f_i = 1\}$. All stations then have to agree on a unique $i^* \in S(\mathbf{f})$ designating the winning slot (and consequently the winner station), or on a no-winner outcome if $S(\mathbf{f}) = \varnothing$. In Fig. 3, $\mathbf{f} = (0\,2\,0\,1\,1\,0\,0)$ and $S(\mathbf{f}) = \{4, 5\}$, therefore $i^* = 4$ or 5. This designates station *3* or station *2* as the winner, respectively.

A unique i^* can be agreed on by defining a deterministic hash function H on the set of possible $\mathbf{f}$. The value returned by H will index into the set $S(\mathbf{f})$ written in ascending order. In the above example, $H(\mathbf{f}) = 1$ would indicate $i^* = 4$ and $H(\mathbf{f}) = 2$ would indicate $i^* = 5$. The function H should have suitable mixing properties. In particular, it should compute to uniformly distributed values for randomly chosen $\mathbf{f}$ and prevent greedy stations from easy guessing of the winning slot based on the observed prefix of $\mathbf{f}$. Of the many possible hash functions, two (denoted H_1 and H_2) have been selected for a closer examination. Let $v(\mathbf{f})$ be the numerical value whose ternary representation is $\mathbf{f}$. Then

$$H_1(\mathbf{f}) = 1 + v(\mathbf{f}) \mod |S(\mathbf{f})|$$

$$H_2(\mathbf{f}) = 1 + round\,[\pi \cdot v(\mathbf{f})] \mod |S(\mathbf{f})|, \qquad (1)$$

where $\pi = 3.14159265358979$, $|\cdot|$ denotes cardinality and *round* symbolises rounding to the nearest integer. Extensive simulation was carried out to evaluate the mixing proper-

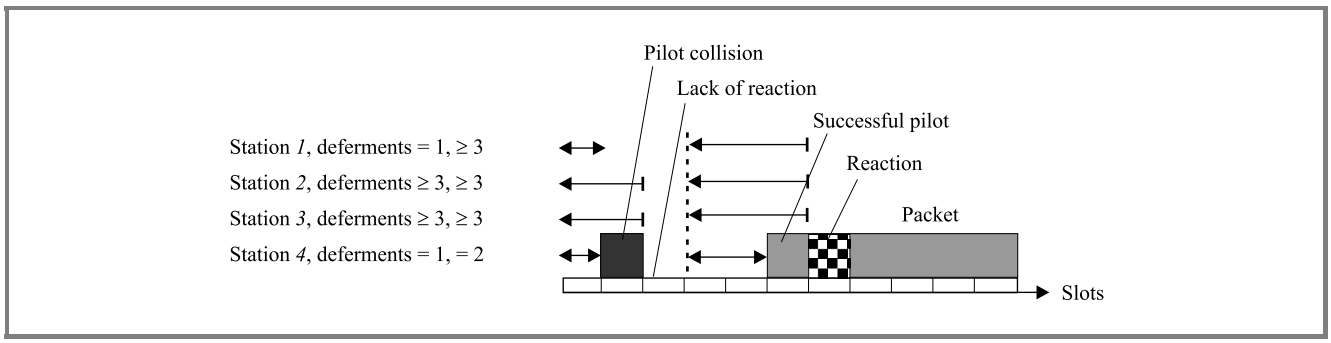

Fig. 1. RT protocol; $N = 4$, $D \geq 4$ (dashed line marks end of protocol cycle).

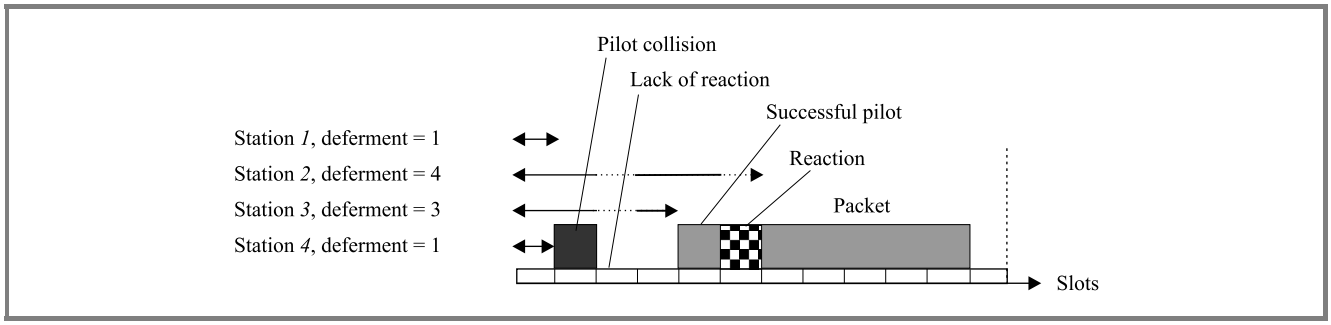

Fig. 2. RT-1s protocol cycle; $N = 4$, $D \geq 4$ (stations *1* and *4* back off, station *3* wins).

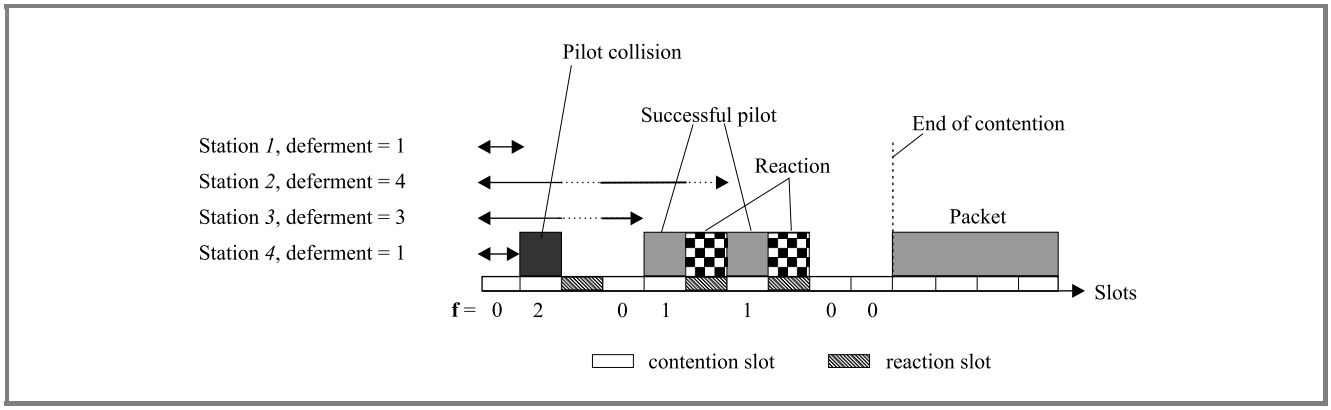

Fig. 3. RT-hash; $N = 4$, $D = 7$.

ties of H_1 and H_2, with each of N stations applying Randomiser. After 1000 instances of contention a histogram *hist* of winning slots was obtained and its normalised entropy was computed:

$$normalised\ entropy = \frac{-\sum_{i=1}^{D} hist(i) \cdot \log_2 hist(i)}{\log_2 D}. \qquad (2)$$

For an ideal hash function, (2) should be close to unity. This was emulated by replacing a hash function by a random number generator (rand). In Fig. 4, H_1 and H_2 are compared to rand in terms of (2); H_2 was found more satisfactory and was taken for further experiments. The results presented in Fig. 4 were generated for $D = 10$; other simulation experiments show little dependence of (2) on D.

Note that the above results are only valid if a station does not have any additional information about the ongoing contention. This need not be the case for a greedy station, which might choose to defer a pilot transmission until a long enough prefix of **f** has been observed. The longer the observed prefix, the worse are the mixing properties of H_2 for the remaining slots. For example, for $D = 10$ the prefix (2 1 0 1 0 2) yields almost even probabilities of winning for the remaining four slots, while (1 2 0 1 0 2) yields 1%, 45%, 12% and 0%. Figure 5 depicts the normalised entropy for the remaining D–L slots, averaged over all L-long prefixes of **f**. One sees that a greedy station in-

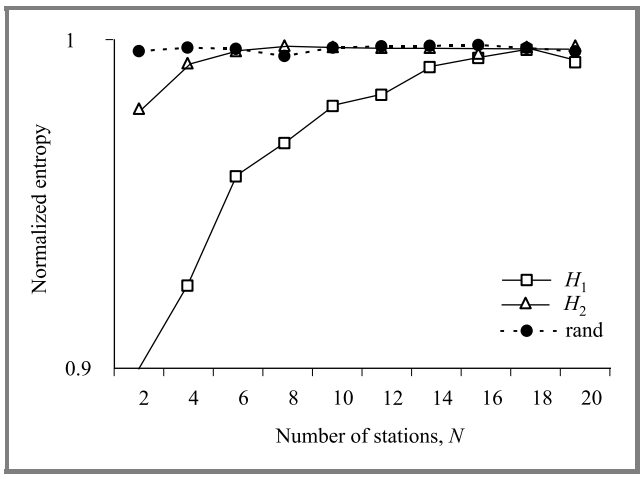

Fig. 4. Mixing properties of hash functions; $D = 10$.

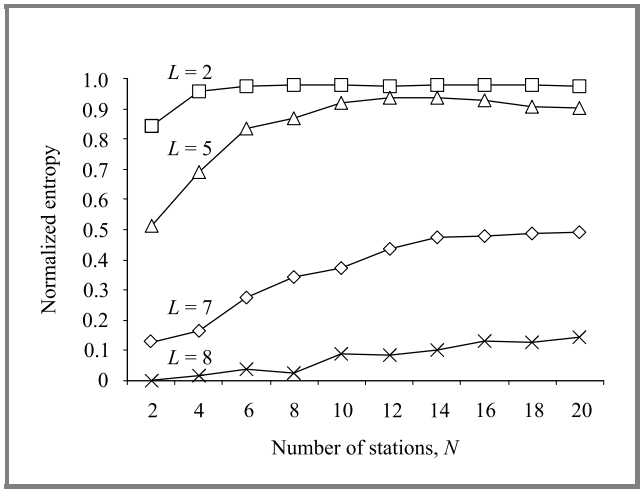

Fig. 5. Mixing properties of H_2 conditioned on L-long prefixes of **f**; $D = 10$ (note the difference in scale compared to Fig. 4).

deed can substantially improve the chances of winning based on the observed prefix. Such an attack is described in Section 4.4.

4. Selection strategies

Greedy stations self-optimise by departing from Randomiser. Because self-optimising strategies do not form a definite set, suitable heuristics should be sought; some are outlined below.

4.1. Aggressive Randomiser

While regular stations use Randomiser, greedy stations may resort to a more "aggressive" probability distribution of deferments, i.e., shifted toward short deferments (Fig. 6). We take it to be a convex quadratic function, namely $\Pr(\text{deferment} = l) = const. \cdot [1 + (l - D + 1)^2]$. The difference between Randomiser and Aggressive Randomiser is

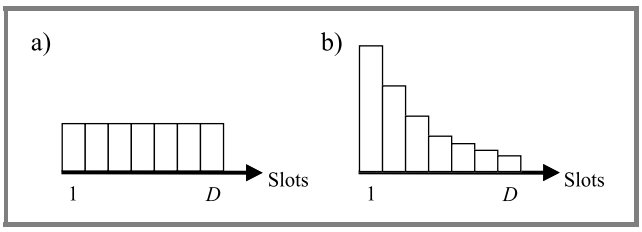

Fig. 6. Probability distributions of Randomiser (a) and Aggressive Randomiser (b).

that the former attempts to optimise the overall bandwidth utilisation, whereas the latter is self-optimising.

4.2. Optimal Randomiser

In the Optimal Randomiser selection strategy, all G greedy stations select transmission deferments at random using a common probability distribution **p** that maximises the bandwidth share they collectively obtain. In numerical experiments, a reinforced random search was applied to determine **p**, starting from a uniform distribution. In each of 10000 steps, 0.05 was tentatively subtracted from one randomly chosen element of **p** and added to another, with the new values only retained if they increased the bandwidth shares of the greedy stations.

Optimal Randomiser violates the isolation constraint since **p** is assumed common to all the greedy stations. It is considered as a worst-case scenario from the regular stations' viewpoint.

4.3. Pseudoperiodic

Suppose the G greedy stations are not subject to the isolation constraint. Firstly, they will arrange to select different deferments to avoid pilot collisions. Secondly, under RT and RT-1s, short deferments will be preferred. For $G = 4$, a strategy in Table 1 may be conceived. Each greedy station defines a deferment sequence for T consecutive protocol cycles and repeats it periodically. In the absence of regular stations this amounts to passing a token from one greedy station to another; the sequence of token holders is also periodic with period $T = 5$. The presence of regular stations may disturb this, but only through pilot collisions in slot 0.

Table 1
Deferments selected by greedy stations in periodic token passing

Greedy	Instants of contention				
	a	*b*	*c*	*d*	e
1	0	3	2	1	3
2	1	0	3	2	1
3	2	1	0	3	0
4	3	2	1	0	2

Under RT or RT-1s, Table 1 exemplifies a Nash equilibrium point [13], i.e., none of the greedy stations can improve its bandwidth share by unilaterally deviating from the specified deferment sequence. The equilibrium is not fair in that the stations are not guaranteed equal bandwidth shares (station *3* will obtain the largest on account of its double 0-slot deferment). Taking only the first four columns and $T = 4$ yields symmetry in the deferment distribution as well as in the obtained bandwidth shares.

The Pseudoperiodic selection strategy aims to reconcile the isolation constraint with the idea of token passing. Each greedy station initially applies a periodic deferment sequence $(s_1 s_2 \ldots s_T)$, $s_i \in \{0, \ldots, D-1\}$, e.g., $s_5 = 3$ means a 3-slot deferment in every 5th protocol cycle. Denote by e_i the currently observed frequency of winning the ith contention. At the end of each period, the e_i's are updated using a low-pass filter:

$$\forall_{i \in \{1,\ldots,T\}} \; e_i = \alpha \cdot e_i + (1-\alpha) \cdot last_i, \tag{3}$$

where $\alpha \in [0, 1]$ and $last_i$ equals 1 if the ith contention was won and 0 otherwise. Subsequently, with a fixed probability, the worst-performing selection is modified, i.e., s_{i^*} is replaced by a new randomly chosen value if $e_{i^*} = \min\{e_1, e_2, \ldots, e_T\}$. Thus Pseudoperiodic permanently improves the obtained bandwidth share.

Technically, the isolation constraint is violated again: the greedy stations have to apply identical T (or its multiple) since lack of synchronisation inevitably leads to more frequent collisions. Nevertheless, the choice of $T = D$ seems natural; one can also imagine a version of Pseudoperiodic with optimisation of T.

4.4. Antihash

The Antihash selection strategy (Fig. 7) was devised to exploit the reduction of the normalised entropy (2) conditioned on the observed prefix. Having observed an L-long prefix $\mathbf{f}_L$ of $\mathbf{f}$, a greedy station uses the statistics of recent

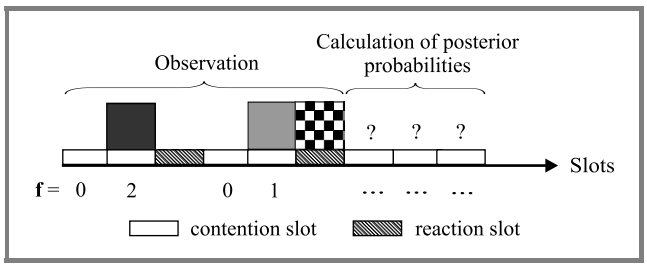

Fig. 7. Antihash; $D = 7$, $L = 4$.

protocol cycles to calculate a posterior probability distribution over possible continuations $\mathbf{f}_{D-L}$ and over the respective winning slots $H_2(\mathbf{f}_L \mathbf{f}_{D-L})$. The most promising slot between the $(L+1)$th and Dth is then determined; if it is not the $(L+1)$th one, the analysis is repeated one slot later with an $(L+1)$-long prefix observed.

5. Performance evaluation

In a series of simulation experiments, regular and greedy stations were contending for access to the medium under heavy load (all stations always had packets ready to transmit). The latter assumption implies concurrent transfer of large files, a perfect scenery for selfish behaviour. In most simulations a fixed number $N = 10$ of stations was assumed, with $D = 10$ and a variable number of greedy stations ($G \in \{0, \ldots, N\}$). Packets were of fixed size $S = 50$ slots.

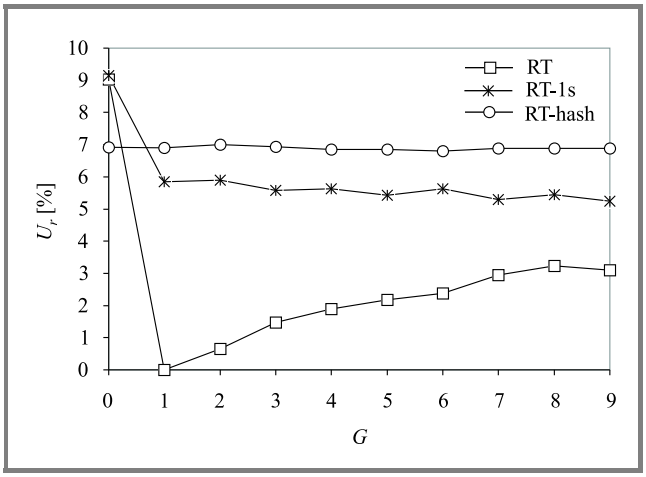

Fig. 8. Optimal Randomiser versus Randomiser.

In Fig. 8, the average regular station's bandwidth share, denoted by U_r, is plotted against G for RT, RT-1s and RT-hash. Regular and greedy stations applied Randomiser and Optimal Randomiser, respectively. $G = 0$ corresponds to an all-cooperative setting; U_r is then slightly lower than $1/N$ or 10% of the channel bandwidth on account of the scheduling penalty; this effect is stronger for RT-hash. In a noncooperative setting ($G > 0$), U_r is even lower under RT and RT-1s. While the former protocol is unacceptable, the latter seems to cope with the presence of greedy stations fairy well, especially when they use Aggressive Randomiser. Unlike RT and RT-1s, RT-hash holds its own regardless of G. Figure 8 can be explained by inspecting the optimal probability distribution $\mathbf{p}$ found by a reinforced random search. They are given in Fig. 9 for $G = 4$. Under RT, $\mathbf{p}$ is strongly biased toward short deferments; under RT-1s this bias is far less visible. Clearly, the more uniform $\mathbf{p}$ the greedy stations arrive at, the less they benefit. In this regard RT-hash is ideal since favouring or discriminating any particular deferment causes more frequent pilot collisions. Thus the selection strategies of regular and greedy stations are identical.

Figure 8 also illustrates a drawback of RT-hash, namely large overhead (as noticed at $G = 0$). This is because each contention lasts until all D contention slots (along with the corresponding reaction slots) have elapsed. For example, $S = 50$ and $D = 10$ result in a 30% overhead; clearly it decreases with S. Additional simulations of RT-hash were

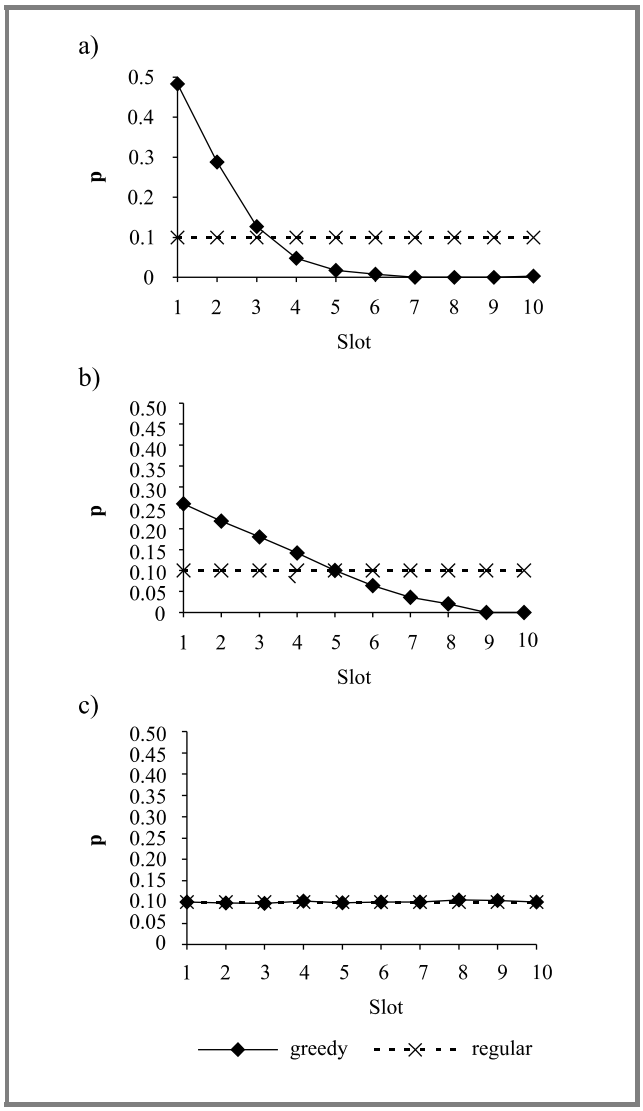

Fig. 9. Probability distribution **p** for Optimal Randomiser; $N = 10$, $G = 4$, $D = 10$: (a) RT; (b) RT-1s; (c) RT-hash.

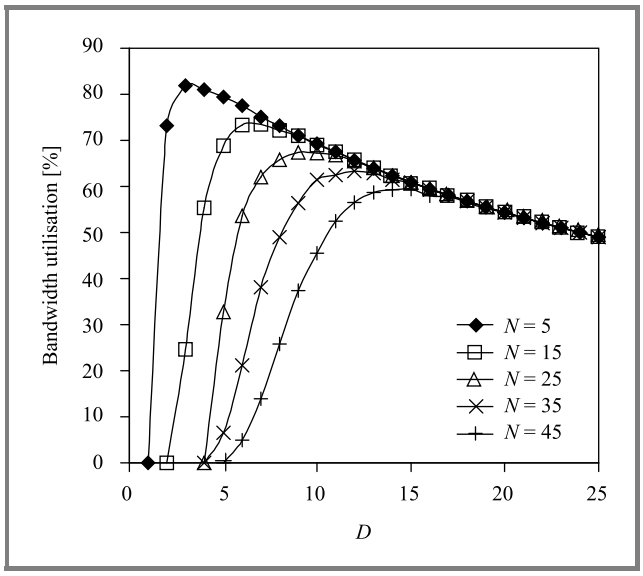

Fig. 10. Bandwidth utilisation under RT-hash.

carried out to determine the overhead under diverse parameter settings ($N = 5..45$, $D = 1..25$); the results are given in Fig. 10. For $N = 10$, the optimal D is equal to 4 and reduces the overhead to less than 20%. Unfortunately there is no uniformly optimal D across various N. A possible solution could be to make D variable and dependent on a current estimate of N, e.g., based on the observed sums $f_1 + ... + f_D$ in recent instances of contention.

In Fig. 11, regular stations used Randomiser, while greedy stations used Pseudoperiodic. For Pseudoperiodic, $T = D = 10$ and $\alpha = 0.95$ were fixed. The latter value implies that the e_i are influenced by the last few dozens of periods. The final deferment sequences at the greedy stations were found to be close to those in Table 1. The greedy stations, none of them having knowledge of the number or status of other stations, managed to establish a token passing sequence.

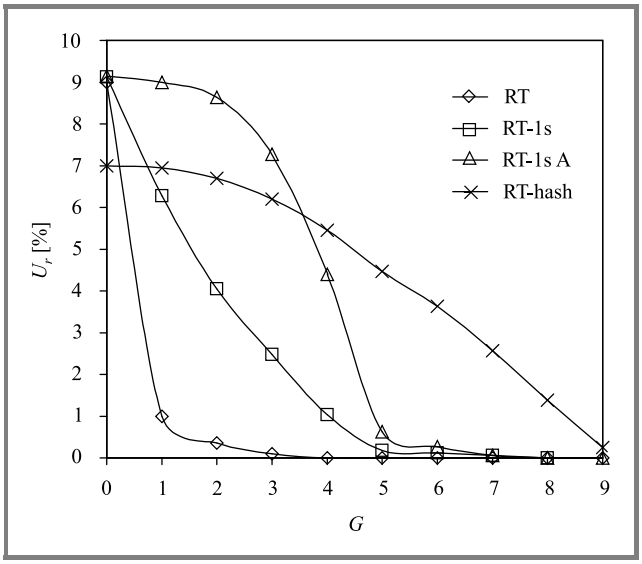

Fig. 11. Pseudoperiodic versus Randomiser.

Observe that as G increases, Pseudoperiodic turns out increasingly beneficial for the greedy stations, reflecting the fact that the token passing scheme inherently avoids pilot collisions, whereas Randomiser does not. However, the benefits depend on the protocol. RT is definitely not resistant to Pseudoperiodic; RT-1s is uniformly superior to RT, although for $G > N/2$ the results are comparably unsatisfactory. The dotted "RT-1s A" line corresponds to Aggressive Randomiser applied at regular stations under RT-1s. A better performance for $G < N/2$ is now observed; still, the range of unfavourable G remains the same. RT-hash prevents regular stations from being cut off even for larger G, at the price of an increased protocol overhead.

In each simulation run, the results presented in Fig. 11 were unfolding gradually. At the beginning, a greedy station's bandwidth share was comparable to a regular station's. Figure 12 shows a sample run under RT-1s. After about 1400 protocol cycles the greedy stations managed to establish a token passing sequence. In general, under all the considered protocols, it took greedy stations fewer

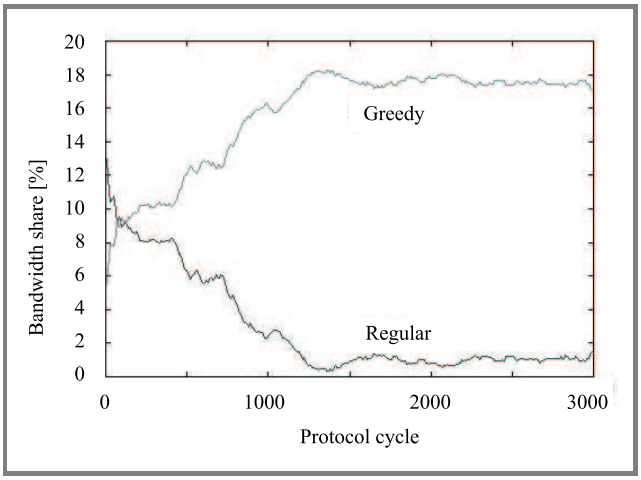

Fig. 12. Pseudoperiodic versus Randomiser under RT-1s; $G = 5$, $N = 10$.

than 2000 protocol cycles to stabilise their bandwidth shares at a high level. With 1500-byte packets and a 10 Mbit/s channel, this translates to less than 3 s. Thus a few seconds' time is enough to threaten regular stations even in changing traffic conditions. This raises the question, if Pseudoperiodic is so effective, could it be adopted as a regular station's standard strategy? The answer is no, for the following reasons:

– Pseudoperiodic is not fair in that the resulting bandwidth distribution heavily depends on the initial deferment sequences; in extreme cases, some greedy stations were observed to perform worse than regular ones,

– under RT-1s, Pseudoperiodic is not resistant to some simple selection strategies, e.g., consistent selection of a 0-slot deferment.

Finally, the performance of Antihash is given in Fig. 13. Note that this strategy might be beneficial only if there is only one greedy station; more would always collide. Therefore in our simulations $G = 1$ was fixed, with N ranging from 2 to 20. For reference, the dashed line indicates a station's bandwidth share if $G = 0$. Due to poor predictibility of the continuations $\mathbf{f}_{D-L}$, Antihash is less beneficial for larger N, though even for $N = 2$ the regular stations are not cut off. Taking a smaller D (discussed before), will make $\mathbf{f}_{D-L}$ even more unpredictable. Therefore Antihash is not a serious threat to RT-hash.

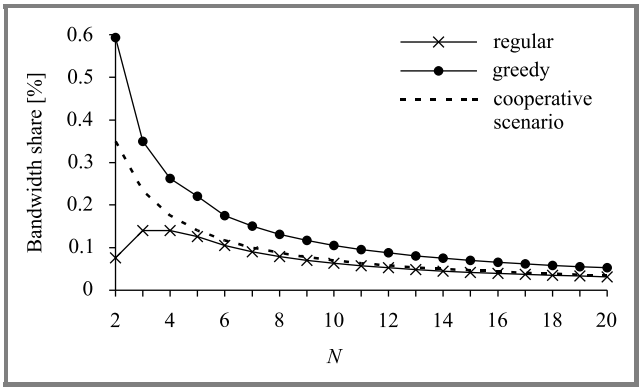

Fig. 13. Antihash versus uniform Randomiser under RT-hash; $G = 1$, $N = 2..20$, $L = 6$, $D = 10$.

6. Conclusion

A new RT-hash MAC protocol for wireless LANs has been proposed to protect regular stations from stations using greedy deferment selection strategies. Two such strategies, Optimal Randomiser and Pseudoperiodic, were considered; the former self-optimises the probability distribution of selected deferments; the latter attempts to establish a token passing-like scheme among greedy stations. RT-hash was simulated in a full-hearability configuration and compared with an earlier RT-1s protocol. Both protocols are comparably resistant to Optimal Randomiser, but only RT-hash is capable of counteracting Pseudoperiodic. A third strategy called Antihash attempted to exploit a potential weakness of RT-hash, but with minor success and only in a very restricted scenario.

References

[1] A. J. Goldsmith and S. B. Wicker, "Design challenges for energy-constrained ad hoc wireless networks", *IEEE Wirel. Commun.*, vol. 9, no. 4, pp. 8–27, 2002.

[2] P. Michiardi, "CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", Res. Rep., Institut Eurecom., 2001.

[3] J. Al-Jaroodi, "Security issues in wireless mobile ad hoc networks at the network layer", Tech. Rep. TR02-10-07, University of Nebrasca-Lincoln, 2002.

[4] L. Buttyan and J. P. Hubaux, "Nuglets: a virtual currency to stimulate cooperation in self-organised mobile ad hoc networks", Tech. Rep. DSC/2001/001, Swiss Federal Institute of Technology, 2001.

[5] I. Chlamtac and A. Ganz, "Evaluation of the random token protocol for high-speed and radio networks", *IEEE J. Select. Areas Commun.*, vol. SAC-5, no. 6, pp. 969–976, 1987.

[6] "Radio Equipment and Systems (RES); HIgh PErformance Radio Local Area Network (HIPERLAN); Services and facilities", ETSI ETR 069 ed. 1 (1993-02).

[7] P. Karn, "MACA: a new channel access method for packet radio", in *Proc. 9th Comput. Netw. Conf. ARRL/CRRL Amateur Radio*, 1990, pp. 134–140.

[8] "IEEE Standard for Information Technology—LAN/MAN—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", ISO/IEC 8802-11, 1999.

[9] J. Konorski, "Packet scheduling in wireless LANs: a framework for a noncooperative paradigm", in *Personal Wireless Communications*, J. Woźniak and J. Konorski, Eds. Boston [etc.]: Kluwer, 2000, pp. 29–42.

[10] J. Konorski, "Multiple access in ad hoc wireless LANs with noncooperative stations" in *Networking Technologies, Services and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications*, E. Gregori, M. Conti, A. T. Campbell, G. Omidyar, and M. Zukerman, Eds., *LNCS*. Berlin [etc.]: Springer-Verlag, 2002, vol. 2345, pp. 1141–1146.

[11] P. Obreiter, B. Koenig-Ries, and M. Klein, "Stimulating cooperative behaviour of autonomous devices—an analysis of requirements and existing approaches", Tech. Rep. 2003-1, University of Karlsruhe, 2003.

[12] P. Kyasanur and N. H. Vaidya, "Detection and handling of MAC-layer misbehavior in wireless networks", Tech Rep., University of Illinois at Urbana-Champaign, 2003.

[13] D. Fudenberg and J. Tirole, *Game Theory*. London, Cambridge (Mass): MIT Press, 1991.

Jerzy Konorski received his M.Sc. degree from the Technical University of Gdańsk (honours) and a Ph.D. degree from the Institute of Computer Science, Polish Academy of Sciences (honours). Since 1985 he has been Assistant Professor at the Department of Information Systems, Gdańsk University of Technology. He is the author of over 30 papers published in international journals or conference records, a co-author of another 10, all in the field of computer networking, and a co-editor of *Personal Wireless Communications* (Kluwer, 2000). His research interests are in performance evaluation, information systems, data transmission, operational research, distributed systems and computer networking. In 1993–96 he lectured at the EFP Franco-Polish School of New Information and Communication Technologies at Poznań and in 1994–96 was a local co-ordinator of a TEMPUS Joint European Project. In 2002 he was awarded the Erskine Fellowship at the University of Canterbury at Christchurch, New Zealand. Since 1995 he has been an IEEE member. Dr. Konorski is a Technical Program Committee member for Polish and Polish-German Teletraffic Symposia and a Scientific Council member at the Maritime Institute in Gdańsk.

e-mail: jekon@eti.pg.gda.pl
Gdańsk University of Technology
G. Narutowicza st 11/12
80-952 Gdańsk, Poland

Maciej Kurant received his M.Sc. degree from Gdańsk University of Technology (honours) in 2002. He is currently a Ph.D. student at the Swiss Federal Institute of Technology in Lausanne (EPFL), Switzerland. His main research interests are in ad hoc self organizing networks, survivability of optical networks and graph theory.

e-mail: maciej.kurant@epfl.ch
Swiss Federal Institute of Technology
CH-1015 Lausanne, Switzerland