A Receiver Based Protecting Protocol for Wireless Multi-hop Networks

Emma Carlson
carlson@tkn.tu-berlin.de

Martin Kubisch
kubisch@ieee.org

Dániel Hollós
hollos@tkn.tu-berlin.de

Telecommunication Networks Group
Technische Universität Berlin
10587 Berlin, Germany

ABSTRACT

Nowadays most medium access protocols designed for wireless ad hoc networks are based on collision avoidance strategies like the CSMA/CA based IEEE 802.11 protocol. But these types of protocols are not designed for multi-hop scenarios – the efficiency of the channel utilization is too low which results in, among others, large packet delays. One popular approach to increase the channel utilization is to reserve time slots along a transmission path, thus having a scheduled access. However, a major problem is interference from nearby nodes, although these nodes are not on the same route. This might lead to destruction of ongoing data receptions. In this paper we suggest a new reservation protocol, called JamTDMA. It offers protection against this effect by advertising the reservations in a larger neighborhood. We will show that this protocol allows to improve the rate of successfully received packets while assuring an upper bound for the end-to-end delay.

Categories and Subject Descriptors

C.2.1 [**Network Architecture and Design**]: Wireless communication; C.2.5 [**Local and Wide-Area Networks**]: Access schemes

General Terms

Protocol Performance and Design

Keywords

Wireless Multi-hop Networks, Reservation Protocol, Receiver Protection, JamTDMA

1. INTRODUCTION

Self-organizing wireless multi-hop networks are a potential means to overcome some of the problems existing in centralized networks. Apart from the ability to work without any fixed infrastructure, they have the potential to increase coverage and throughput [11]. In these networks, all nodes must cooperate in making decisions about when to transmit. One popular method is to use a carrier sensing based Medium Access Control (MAC) mechanism; by sensing the channel idle, nodes can transmit. Well-known and broadly used is the IEEE 802.11 standardized group of MAC protocols [6]. This protocol gives a sufficient support for the best effort type of traffic, e.g., email or web browsing in lowly loaded, sparsely populated systems.

In networks with a large number of nodes, which is desirable for well-functioning multi-hop scenarios and higher traffic loads, it does not perform accordingly [19, 8]: The time that a node waits and avoids a transmission consumes most of the bandwidth. The reason being that a node listens to the channel for *potential* interference which *could* destroy a successful data exchange. Such a protecting mechanism is surely necessary in the direct neighborhood where a node can *decode* any packet transmitted. Hence, it would create strong interference at the intended receiver. But it is not obvious how sensitive this listening must be when the node does not decode the packets anymore and only detects the power or the presence of a signal.

In scenarios where the listening is too sensitive, i.e., a wide area around the node must be silent, it could be entirely possible that two transmission take place at the same time. These transmission would surely reduce each others signal-to-interference ratio, but the remaining ratios *at the receiver* are still high enough for a successful decoding of the packets. Thus, simply listening to the channel is not appropriate to determine whether an additional transmission would reduce the *receivers signal-to-interference ratio* such that they are unable to decode the packets. This is especially difficult for multi-hop networks where a key component is the spatial reuse of the channel to preserve bandwidth.

Even Quality-of-Service (QoS) requiring traffic types, e.g., real-time transmissions, do not function well in a multi-hop environment with the 802.11 MAC protocol [5]. One means to overcome this problem is to reserve resources, i.e. time slots, along the multi-hop path, from source to destination, removing the uncertainty inherited by the IEEE802.11 MAC protocol. Typically, the channel is divided into pre-defined slots. Nodes learn from listening to these slots and other announcements from their direct neighbors whether these slots are available or not.

Having this information a node can making reservation (TDMA on top of CSMA). However, these protocols suffer

PE-WASUN'05, October 10–13, 2005, Montreal, Quebec, Canada.

from the same problem as described above: The CSMA approach of protection ongoing transmissions does not fit well to the gradually decrease of power in the wireless medium. Neither is the position of the active receiver known nor can the signal-to-interference ratio at the position of the active receiver be determined.

As we show in this paper, the needed protection around a receiver can be determined assuming an acceptable packet-error rate. This protection is beyond the direct neighborhood, but still within a two-hop neighborhood around a receiver. According to these results, we propose a new TDMA based reservation protocol, *JamTDMA*, which firstly provides a two-hop protection around the receiver, secondly combines multiple mechanisms in a novel way to achieve this, and thirdly has an upper limit on end-to-end delay (any synchronous TDMA system is more desirable for achieving a low bound on delay). The downside of a TDMA based system is the need of a common understanding of time. Nevertheless, this can be achieved with higher level synchronization algorithms [15, 16] and we assume that a proper algorithm is in place.

In Section 2 we describe related work and the flow reservation protocol with which we compare JamTDMA. In Section 3 we formally show that the receivers need to be protected *beyond* their communication range. Section 4 describes the JamTDMA protocol and Section 5 its performance analysis. Finally, we give a conclude of this paper in Section 6.

2. RELATED WORK

Several extensions and modifications of the IEEE 802.11 MAC protocol Distributed Coordination Function (DCF) have been proposed over the last years. In [9, 17, 7] different types of reservation techniques are introduced which extends the CSMA mechanism by either letting nodes reserve for future packet transmissions or by reserving a certain (sub-)bandwidth. However, when a *periodic* reservation is needed to meet stringent requirements, a better approach is to use fixed schedules in a TDMA-based fashion [4, 14].

Fang et al. developed the MAC-RSV protocol [4]. This protocol is TDMA-based and separates the control phase and the data phase. A node that wants to transmit data in the upcoming data phase sends a request (RTS) in a mini slot of the control phase and waits for a clearance (CTS) in the next mini slot. Upon receiving the CTS, the transmitter sends a confirmation (CONF) message in the subsequent mini slot, thereby informing surrounding nodes that the reservation was successfully established. Thus, every reservation set up phase consists of a mini slot triplet.

Surrounding nodes that overhear an RTS can object if they have a conflicting reservation by transmitting a negative confirmation (NCTS) in the mini slot dedicated to a CTS transmission, thus destroying (or jamming) the reception of a CTS from the intended receiver. But as it is important to protect a reception and not its transmission (the interference at a receiver can destroy a successful reception, a sender does not care), MAC-RSV has a flaw: Surrounding nodes, aware of a conflicting reservation, can only jam when they overheard the RTS. If a node is located in such a way that it only overhears the CTS, it cannot stop a conflicting reservation. Thus, MAC-RSV does not provided the required symmetric protection around a receiver. Instead, it creates a protect around the sender, though possibly unneeded. Throughout this paper, we use MAC-RSV as a reference protocol for our simulative investigations.

Another interesting feature of reservation protocols is jamming. In [20], an additional channel – needed for reservation negotiation – is jammed when necessary. As long as the receiver is receiving data it jams this channel. Thus, it prevents other nodes from negotiating a second transmission in the vicinity of the receiver.

Although this procedure achieves the needed receiver protection (for the costs of a *separate channel* solely used for reservation negotiation), the approach suffers from a similar problem as described in 1. The jamming signal is only recognized as energy of some possible interferer. Thus, it might influence larger areas than necessary in many cases: It is not clear beyond which distance the signal blocks any parallel transmission which could be permitted when the signal-to-interference ratio is taken into consideration.

3. ANALYSIS

We are interested in the range around a receiver, in terms of hops, in which the other nodes should participate in the decision about an intended transmission. We consider the scenario shown in Figure 1; assume that node B has successfully scheduled a data transmission towards node A being d distance away (i.e. an RTS-CTS-like handshake is done). The question under investigation is the minimal distance s of the interfering node C from A so that the Packet Error Rate (PER) at node A is still acceptable. This will tell us how far we have to distribute the information before deciding about the acceptance of a new schedule.

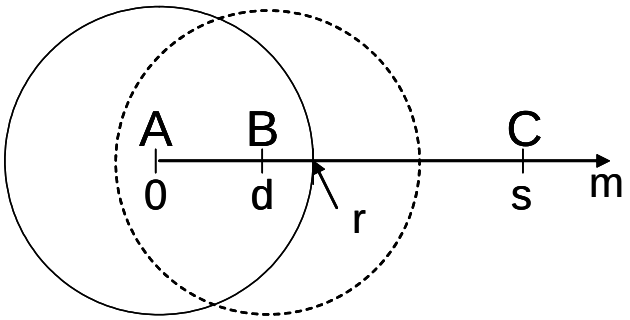

Figure 1: Basic scenario

3.1 Assumptions

We use the basic 1MBps modulation modus of 802.11b with differential binary phase shift keying (DBPSK) for both the control- and data transmission phases. We set the receiver sensitivity to -87 dBm which is common for currently deployed transceiver [13]. All nodes transmit with maximum power of 100 mW. The *radio range* is defined as the maximal interference range of a node; its value is implicitly given by the range where the received power equals or is greater than the background noise, chosen as -111 dBm [2].

We define the *communication range* r as the distance in which a node can successfully receive a packet in case of no interference. All nodes have uniform communication range and use the frequency of 2.4 GHz. In our model we assume a path loss coefficient of three, and a maximal acceptable packet loss rate (PER) of 5 %.

3.2 Calculations

Applying the simple link budget [21] calculations, the communication range for our model is $r = 45$ m. First, we calculate the PER at node A with varied interfering distance $s = 45, 75, 90, 120, 145$ m.

$$\text{PER} = 1 - (1 - \text{BER})^{size}$$

where $\text{BER} = \frac{1}{2}e^{-\frac{E_\text{b}}{N_0}}$ is the bit error rate for DBPSK modulation. $\frac{E_\text{b}}{N_0}$ is calculated from:

$$\text{SINR} = \frac{E_\text{b}}{N_0} \cdot \frac{R}{\text{BW}} = \frac{P_\text{RBA}}{P_\text{RCA} + N_0}$$

where P_RBA is the received power at B by node A, P_RCA is the received power at A by the interferer node C; BW is the bandwidth and R is the transmission rate. The resulting PER curves are shown in Figure 2. The results for $s > 90$ m are omitted because the PER was 0 % in these cases.

Figure 3 shows the dependency of the minimal allowed interfering distance s versus the distance of the communicating peers d.

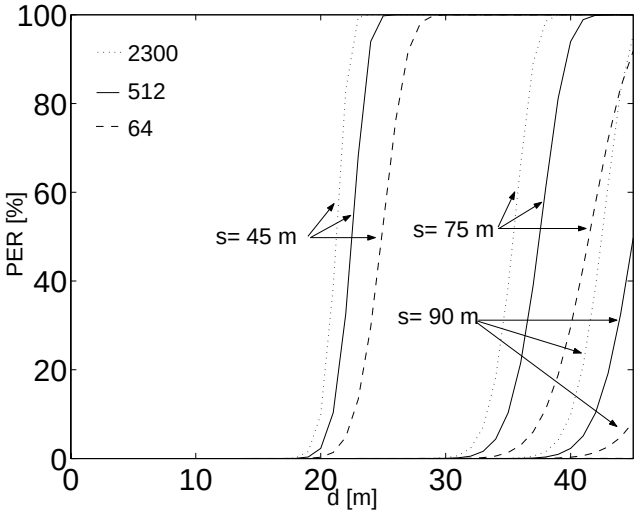

Figure 2: PER with $s = 45$ - 90 meters and packet sizes of 64, 512 and 2300 bytes

The two dotted lines mark the distances where $s = r$ and $2r$ respectively. The results show that the minimum required s falls between r and $2r$ for the majority of the cases which suggests that it is sufficient to protect the receiver in a two-hops range. There is only a tiny interval 42 m $< d < r$ which requires three-hop protection. In the following section we show that a two-hop protection is indeed an acceptable compromise.

3.3 Required two-hop protection

In cases the acceptable s is outside, we here introduce the distance a. This distance is the part of the unacceptable s outside $2r$ (and does not belong to b, which between r and $2r$ of the receiver). The nodes in our cell are uniformly placed (circular influence area with radius responding to the influence level, see Section 3.1). Thus, the parts a and b of

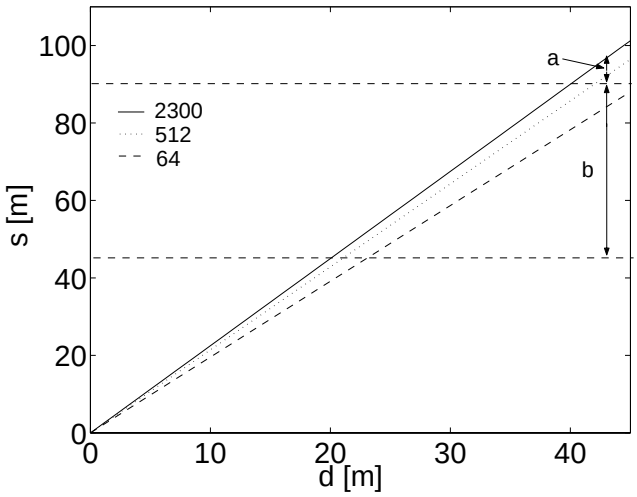

Figure 3: Acceptable s for a PER of 5 % and packet sizes of 64, 512 and 2300 bytes

the unacceptable s distances for all packet sizes result in problematic annulus areas, each spanned by either a ($s > 2r$) or b ($r < s < 2r$). For these annulus the interfering node does not retrieve information about the transmission that will take place.

Figure 4 shows the probabilities that the interferer C is within this annulus. It implies that the probabilities of a packet error is larger than 5 % for any node in this region, i.e., the node is located outside the communication range of node B, while still in the two-hop radius or even outside of the two-hop radius.

As the nodes are uniform randomly distributed, the probability that a node is within a certain region is simply the area of that region divided by the total cell area. In Figure 4, we show three lines for the probability: First the PER is larger than 5 % and the interferer is outside the communication range r (total probability). Second the PER is larger than 5 % and the interferer is outside r but within $2r$. Third the PER is larger than 5 % and the interferer is outside $2r$.

The acceptable s is within $2r$ as long as the distance between the receiver and the transmitter is not larger than 40 meters. These results remain valid, independently from the packet size. Furthermore, the probability that a node at this position has an s which is within a two-hop communication radius is much larger than the probability that the node is located outside $2r$.

Hence, we can conclude that by introducing a two-hop protection we can reduce the number of possible interferer (which could cause a PER larger than 5 %) by 80 %. That means that using a simple RTS/CTS exchange (which protects the one-hop neighborhood of a communication) as a way to prevent an interferer from disrupting a reception is not enough. For scenarios where more interferer are present, this is even more critical, as described in Section 5.

4. THE JAMTDMA PROTOCOL

4.1 Qualitative description

According to the results of our analysis, we designed the medium access protocol – JamTDMA. This protocol ensures

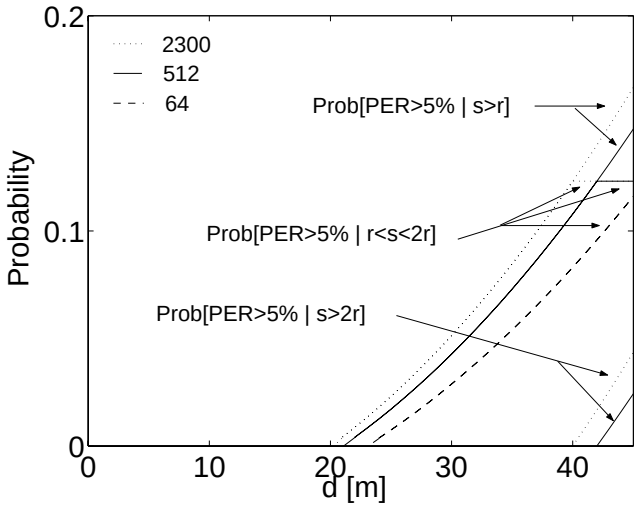

Figure 4: Probabilities that an interfering node is located within one of the annulus' and causing a PER larger than 5 %

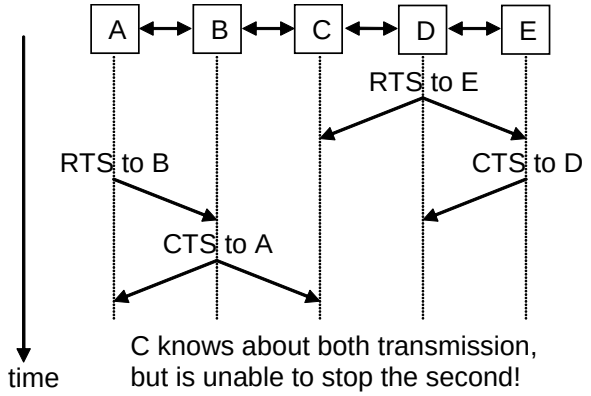

Figure 5: Timing problem of information distribution

that no parallel transmissions take place within a two-hop neighborhood of any *receiver* and our TDMA structure is designed for long-term periodic data slot reservations. As proposed by others [4, 12, 10], we keep the control phase and the data transmission phases separate. With the help of this separation and the two-hop protection, an unique assignment of slots in the data phase can be achieved. Thus, no collision is expected for packet transmissions in this phase. Further on, as nodes need their transceiver only for the control phase or when involved in a data transmission, they can switch it off for the remaining time – an option not possible in CSMA systems. Hence, with JamTDMA nodes can reduce their total energy consumption, which is especially important in networks of battery driven nodes.

Another problem which exists in current reservation protocols [4, 20], is likely to occur (depict in Figure 5): Node C is informed about an data exchange between D and E, but it is not able to block a reservation for the same data slot (between A and B) in its two-hop neighborhood. Node C is only informed about a reservation, but can not object (only hears the CTS).

In order to resolve this problem, the neighbors of B need to check their allocation vectors and object in case of assignment collisions. In JamTDMA we modified the reservation mechanism of MAC-RSV to resolve this problem: A node, after receiving a reservation request, re-announces this request to its neighbors. The neighbors check for already granted reservations in their own neighborhood and object in case of a reservation collision. When no neighbor reports a collision, a node is safe to assume that the requested slot is not used in a two-hop neighborhood. As multiple neighbors can report such a possible collision, a jamming signal (which can be safely discovered, even when overlapping) is used to inform about collisions. While such a jamming can also have a reach beyond the one-hop neighborhood, it is only used in a certain *context*. Jamming is only used in the control phase to destroy the successful reception of a confirmation and not to block any station from trying to establish a reservation. Thus, it does not suffer the problem mentioned in Section 1.

Using these mechanisms, JamTDMA creates a symmetric protection in an area where it is needed – around the receiver.

In order to reduce the required time for a reservation, we use different priorities for different control messages. The higher the priority, the earlier a messages is issued (due to the TDMA structure of our protocol, we can safely assume that all nodes know the correct state of the channel). By giving a jamming signal the highest priority, we assure that all neighbors can object and prevent a confirmation from being delivered. Further, the confirmation and the reannouncements have a higher priority than the requesting message, i.e., no new reservation request can disturb an already ongoing reservation setup.

4.2 Functional description

4.2.1 Data slot reservation

We extend the MAC-RSV [4] protocol as described in Section 4.1. Recall that MAC-RSV is TDMA-based, i.e., the time is divided into *frames*; each frame consists of a control phase and a data phase. In the control phase all necessary negotiations are performed to ensure that a data transmission is free of any collision. These negotiations divide the control phase into *mini slots* (a sub-TDMA structure). Each mini slot is capable of transmitting one MAC control message; the addressed receiver(s) of those control messages respond in the next mini slot. The MAC-RSV protocol uses three such mini slots for each intended transmission to ensure that the one-hop surrounding of the sender-receiver pair is informed (see RTS-CTS-CONF triplet described in Section 2).

Our JamTDMA protocol shifts the protection towards the receiver by enabling its two-hop neighbors to *object* any intended transmissions. For the protocol description assume that node A needs to reserve a data slot for transmission to node B. Then the protocol steps are as follows: First, node A randomly picks a mini slot n for the transmission of an RTS. The RTS message (apart from the standard content of sender and receiver address) contains an indicator of the randomly chosen data slot to be used for the actual data transmission. In the next mini slot $n+1$ node B reannounces this information to its neighbors with the help of

a *request for acceptance* (RFA) message. Then, in mini slot $n+2$ node B can reply, when non of its neighbors object (any node that receives either the RTS or the RFA packet can object if it is aware of a potentially conflicting slot allocation) with the help of a jamming signal. We assign the *highest priority* to those jamming signals: If any node issues a jam signal and node B can recognize it, node B is not allowed to send the CTS (see Section 4.2.2).

If there is no objection, node B may accept the request and respond with a CTS message in mini slot $n+2$. Node B may reject the request by not transmitting the CTS if the chosen data slot was already occupied in its own allocation table. In this case node A will miss the CTS and will try the same procedure choosing another data slot.

The JamTDMA protocol uses the same number of mini slots to perform reservations as the MAC-RSV. However, unlike the MAC-RSV, the one-hop neighbor of the sender will not be notified whether the data slot reservation was successful or not. Instead, JamTDMA achieves that the two-hop neighborhood of the receiver refrains from using this slot. Additionally, as the release of an unused slot is necessary in a reservation protocol, we introduce the keep-alive mechanism, described in Section 4.2.3.

4.2.2 Priorities

The priorities are implemented exploiting the synchronous mini slot structure. The beginning of these slots is synchronized among the nodes. A high-priority message in a mini-slot is transmitted earlier than a lower priority message (see Figure 6). The time must be sufficient to allow a node with a low priority message to detect a busy mini-slot. Hence, each node willing to transmit a lower priority control message must listen to the channel before it can transmit.

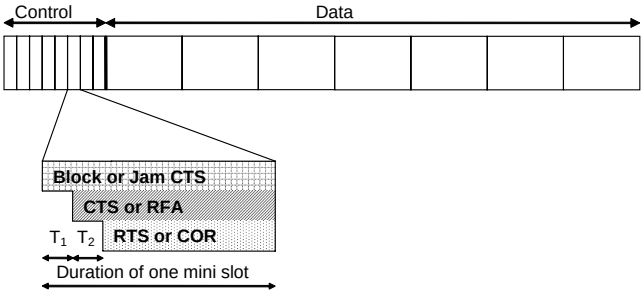

Figure 6: Frame structure

The priority order of the control messages is set as follows: The jamming signal is transmitted directly at the start of a mini slot, thus having the highest priority. The CTS/RFA is delayed so that nodes can detect the jamming signal by carrier sensing. Finally, the RTS is delayed such that it has the lowest priority.

4.2.3 Acknowledgement protocol

Data packets in our scheme are not acknowledged explicitly. Instead, the presence of the *data path* (i.e. the link between the nodes) is checked periodically. The receiver of any scheduled data transmission periodically issues a special message called *confirmation of reservation* (COR) in one of the mini slots of the control phase. This informs surrounding nodes whether a reservation is still active. The COR messages have the same priority as the RTS messages, as can be seen in Figure 6.

If a node is part of a multi-hop flow reservation, the COR messages are also used as *path alive* signals, e.g., for recognizing whether the reservation path is broken and/or requires path maintenance [1]. A simple maintenance algorithm for further exploiting the COR messages is as follows: If a node detects a link failure in a multi hop data path and is not able to repair it locally, it stops sending the COR messages. Thus, an implicitly delegation of the reparation task to the preceding node is done. This procedure is repeated as long as the flow is not repaired or the reparation task is delegated to the original sender, eventually informing the original sender of a disrupted path.

4.2.4 Rejection of reservation

A node rejects a new reservation attempt when the requested data slot is occupied. In such a case the sender node should retry and request another data slot in the upcoming RTS message. However, the situation might be different for the case when all data slots for the intended receiver are occupied. Thus it is no worth trying it again. In order to be able to separate this two cases, the receiver node may send a CTS message to node A with NACK to signal that no more data slots are available. If this happens, a new path setup can be started along a different path or the reservation may be retried after some time, assuming that other paths are deleted by that time. This is not further investigated in this paper, but is suggested for further work.

4.2.5 End-to-end delay

When a reservation is established for a multi-hop path (involving multiple forwarding hops), each packet has a fixed transmission/reception time. Thus the end-to-end delay is constant and there is no jitter induced by the protocol. The end-to-end delay itself depends on the data slot a node can reserve for the transmission. In the best case all data transmission slots of the whole paths are reserved directly after another. Assuming the number of hops of a path is N and the slot size is S, the minimum end-to-end delay would then be $N \cdot S$.

The maximum delay one node of the chain can cause is that it can only reserve a data transmission slot in the frame, which is directly before the slot used for reception. Thus, the maximum delay (the upper bound of the end-to-end delay) is: $N \cdot (F - S)$, where F is the frame duration. When the end-to-end delay is too long for a certain QoS, the reservations should be released. Then the resources can be reused by other nodes and the source node could try again. Thus, a more suitable slot reservation pattern could be found for the whole path.

5. SIMULATION RESULTS

For evaluation of our JamTDMA protocol, we performed simulations using the OMNeT++ simulation system [18] and the mobility framework [3]. In this simulation environment, the signal-to-noise-and-interference ratio and the signal power are determined at a receiver at any time. When the SNIR (dependent on the required packet-error rate) is too low or the required signal power (given by the receiver sensitivity of the transceiver) is fallen short during a reception process, the received packet is considered as erroneous. The underlying model takes all powers concurrently radiated

at any time into account when deciding whether a packet was successfully received or not. Thus, it is closer to reality than a discrete model, i.e., with disks of communication and disturbance areas.

The parameters for the simulation comply to our analysis with -87 dBm receiver sensitivity, a noise level of -110 dBm, a carrier frequency of 2.4 GHz, a limited transmission power of 2 mW, a bit rate of 1 Mbit/s and packet lengths between 512 and 2300 bytes. Furthermore, we used a JamTDMA frame duration of 300 ms with a control phase of 3 ms and a priority waiting time according to one data symbol.

The nodes in our network are deployed in a line and a grid fashion. For the line scenario we use six nodes and the packets are create at the first node. They need to traverse the four following nodes before they reaches the last node – their final destination. In the grid scenario the nodes are located such that we have two or six such lines and all nodes are equally spaced. As the traffic is always from the first node of a line to the last, we end up having one, two and six flows, respectively.

An additional parameter in our simulation is the spacing between the nodes. The distance is varied relative to the possible radio range (CR – defined by receiver sensitivity) and ranges from $0.5 * CR$ to $1 * CR$. A value larger than CR would result in a line/grid which is not connected. A value smaller than half CR would neglect the next node as a hop, thus the communication in the line/grid could use fewer hops.

Figure 7 shows the rate of successfully received packets for a path loss coefficient of two (all pictures are with an confidence level of 95 %). The lowest curve in the picture is

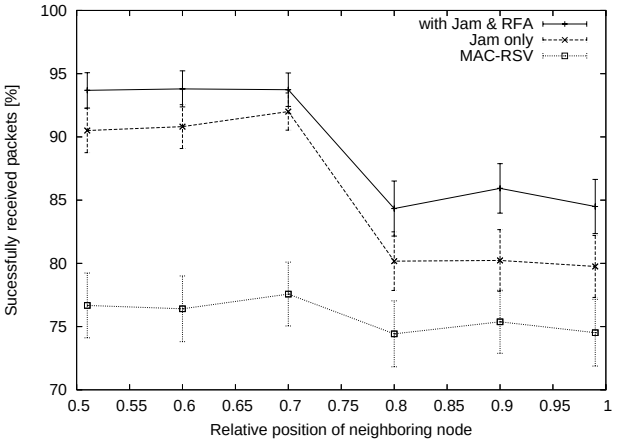

Figure 7: Comparison of successfully received packets

the rate of successfully received packets when no jamming is in use (for this case the JamTDMA protocol has a similar behavior as the MAC-RSV [4]). Thus, the receiver has only a one-hop protection. The middle curve shows the successfully received packets when jamming but no RFA is used and the upper curve is for jamming and RFA. It is interesting to note that with a spacing value larger than $0.75 * CR$ a sudden drop happens, as this is the distance when the important diagonal node is out of communication reach. Thus, this node is unable to receive the announcements and can not jam conflicting slot allocations. However, as we used a layout of nodes to explore this border case problem, it is unlikely to have a large impact in networks of randomly placed nodes.

Figure 8 shows the possible gain over the number concurrent flows. The different curves represent different path loss coefficients used. It is interesting to note that the achievable

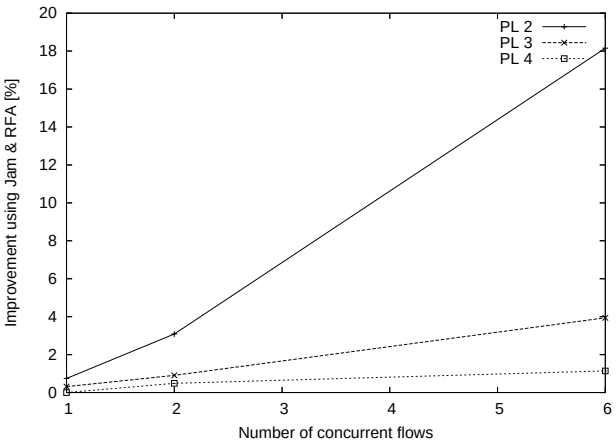

Figure 8: Gain using Jam and RFA

gain strongly depends on the path loss coefficient – higher coefficient values reduce the possible gain. This reduction of gain is due to the fact that systems without jamming perform significantly better with a higher path loss coefficient. That in turn means, that with a two-hop protection around a receiver a system is less sensitive to changes in path loss. Thus, is is more stable in harsh environments with changing channel behavior. While our simulation was only performed for up to 36 nodes, we expect higher gains in larger networks where the interference is much stronger.

Finally, Figure 9 depicts the end-to-end delays for the different MAC protocols, where the x-axis shows the number of flows used and the y-axis is the induced end-to-end delay. The highest line shows the end-to-end delay for the initial packet when JamTDMA is used. The second line shows the delay using MAC-RSV, and the lowest line shows the end-to-end delay of an established JamTDMA flow.

The initial JamTDMA packet needs more time than MAC-RSV, as a more complex slot reservation mechanism is used. But as soon as the established path is followed, we have a very low and constant packet delay. When we apply the frame duration and the number of hops involved to the calculation of Section 4.2.5 ($N = 5$ hops, $F = 300$ ms, $S = 4.5$ ms), we obtain a maximum end-to-end delay of 1.46 s for an established path. This corresponds quite well to our simulation: The value was not exceeded in the simulation, and the average end-to-end delay has an expected value of $\frac{1}{2}$ of the maximum end-to-end delay (which can be seen in Figure 9).

While the results are according to our expectations, it is interesting to note that an increasing number of concurrent chains (2 versus 6) does not dramatically increase the *end-to-end delay of the initial packet*. This might be different in scenarios with higher load, but as this requires an adaptation of control phase and data phase (the end-to-end delay for

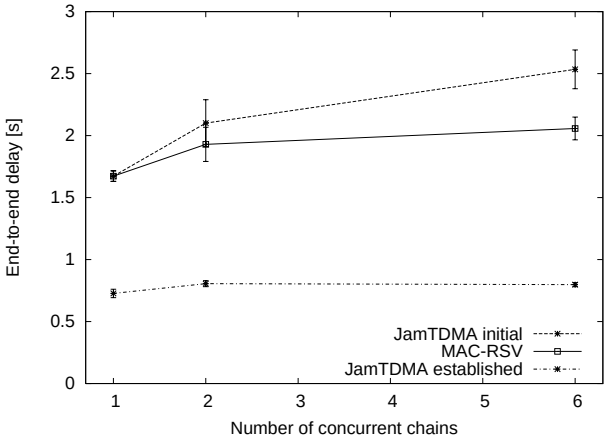

Figure 9: Comparison of end-to-end delay

the initial JamTDMA packet and MAC-RSV solely depends on the slots available in the control phase), we leave the discussion of throughput optimization for further studies. However, when the end-to-end path is established, the delay is constant for this path. Only when the network is close to saturation, JamTDMA rejects the creation of new paths.

6. CONCLUSION

For delay and quality-of-service sensitive applications in multi-hop networks, e.g., voice transmission in mesh networks, it is important to have a predictable and highly reliable packet delivery. Possible candidates for achieving the aim are from the class of TDMA protocols. With such a protocol it is also possible to separate the control and the data phase of a node-to-node communication, which, as a side effect, can be helpful in reducing idle-listening time for energy constrained networks.

Additionally, as was shown in the paper, a two-hop protection around a receiver is necessary in multi-hop wireless communication systems. To enable such a two-hop protection, a separation between control and data phase is highly efficient and easy to implement; extending the protection during the control phase does not interfere with the data transmissions.

Having learned this, we propose a new MAC protocol – the JamTDMA. It extends the RTS/CTS exchange and achieves the required two-hop protection using the – *jamming on behalf of others* – approach. Applying this principle does not create too much overhead as it only increases the, anyway necessary, reservation procedure by one message compared too IEEE 802.11 and is equal too MAC-RSV. But the gain is a reduced packet failure rate (in our simulations by up to 20 %), leading to less retransmissions.

Apart from the reduction of number of retransmissions it is also necessary to have a predictable end-to-end delay. This is also achieved by the use of a special signalling in JamTDMA. Thus, the required end-to-end delay for a given network can be achieved by choosing the frame time of JamTDMA according to the number of hops involved.

7. REFERENCES

[1] E. Carlson, C. Bettstetter, H. Karl, C. Prehofer, and A. Wolisz. Distributed maintenance of resource reservation paths in multihop 802.11 networks. In *Proc. of Vehicular Technology Conference (VTC Fall)*, Los Angeles, California, USA, Sept. 2004.

[2] S. Desilva and R. V. Boppana. On the impact of noise sensitivity on transport layer performance in 802.11 based ad hoc networks. In *International Conference on Communication (ICC)*, Paris, France, June 2004. IEEE.

[3] W. Drytkiewicz, S. Sroka, V. Handziski, and A. Köpke. A Mobility Framework for OMNeT++. Technical report, Telecommunicaton Networks Group, Technische Universität Berlin, 2003.

[4] J. C. Fang and G. D. Kondylis. A synchronous, reservation based medium access control protocol for multihop wireless networks. In *Wireless Communications and Networking Conference (WCNC)*, New Orleans, LA, USA, Mar. 2003. IEEE.

[5] M. Gerharz, C. de Waal, M. Frank, and P. James. A Practical View on Quality-of-Service Support in Wireless Ad Hoc Networks. In *Proc. of the IEEE Workshop on Applications and Services in Wireless Networks (ASWN)*, Bern, Switzerland, July 2003.

[6] IEEE Standard Department. *IEEE 802.11 Standard for Wireless LAN, Medium Access Control (MAC) and physical layer (PHY) specifications*. IEEE, New York, NY, USA, 1997.

[7] S. Lee and A. Campell. INSIGNIA: In-band Signalling Support for QoS in Mobiloe Ad Hoc Networks. In *MoMuC*, Berlin, Germany, Oct. 1998.

[8] J. Li, C. Blake, D. S. J. D. Couto, H. I. Lee, and R. Morris. Capacity of ad hoc wireless networks. In *International Conference on Mobile Computing and Networking (MobiCom)*, Rome, Italy, July 2001. IEEE.

[9] C. Lin and M. Gerla. Asynchronous multimedia multihop wireless networks. In *INFOCOM — The Conference on Computer Communications*. IEEE, Apr. 1997.

[10] M. Marina, G. Kondylis, and U. Kozat. RBRP: a Robust Broadcast Reservation Protocol for Mobile Ad Hoc Networks. In *Proc. IEEE Intl. Conf. on Communications (ICC)*, Amsterdam, Netherlands, Jun 2001.

[11] S. Mengesha and H. Karl. Relay Routing and Scheduling for Capacity Improvement in Cellular WLANs. In *Proc. Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)*, Sophia-Antipolis, France, Mar. 2003.

[12] M. J. Miller and N. H. Vaidya. On-demand tdma scheduling for energy conservation in sensor networks. Technical report, University of Illinois at Urbana-Champaign, Urbana, IL, USA, June 2004.

[13] Nordic VLSI ASA. *nRF2401 Single Chip 2.4GHz Radio Transceiver*. Tiller, Norway, Mar. 2003.

[14] V. Rajendran, K. Obraczka, and J. Garcia-Luna-Aceves. Energy-efficient, collision-free medium access control for wireless sensor networks. In *Conference On Embedded Networked Sensor Systems (SenSys)*, Los Angeles, CA, USA, Nov. 2003. IEEE.

[15] K. Römer. Time synchronization in ad hoc networks. In *International Symposium on Mobile Ad Hoc Networking and Computing - MobiHoc*, pages 173 – 182, Long Beach, CA, USA, Oct. 2001. IEEE.

[16] M. L. Sichitiu and C. Veerarittiphan. Simple, accurate time synchronization for wireless sensor networks. In *Wireless Communications and Networking Conference (WCNC)*, New Orleans, LA, USA, Mar. 2003. IEEE.

[17] J. Sobrinho and A. Krishnakumar. Real-time traffic over the ieee 802.11 medium access control layer. In *Bell Labs Technical Journal*, volume 1, pages 172–187, Autumn 1996.

[18] A. Varga. *OMNeT++: Discrete Event Simulation System*. Technical University of Budapest, Faculty of Electrical Engineering and Informatics, Budapest, Hungary, 2.1 edition, Mar. 2001.

[19] S. Xu and T. Saadawi. Does the IEEE 802.11 MAC protocol work well in Multihop Ad Hoc Networks? June 2001.

[20] S.-R. Ye, Y.-C. Wang, and Y.-C. Tseng. A jamming-based mac protocol to improve the performance of wireless multihop ad hoc networks. *Wireless Communications and Mobile Computing (SCIE)*, 4:75–84, 2003.

[21] J. Zander and L. Ahlin. *Principles of Wireless Communications*. Studentlitteratur, Sweden, 1998.