Problems with Correct Traffic Differentiation in Line Topology IEEE 802.11 EDCA Networks in the Presence of Hidden and Exposed Nodes*

Katarzyna Kosek[1], Marek Natkaniec[1], Luca Vollero[2]

[1] AGH University of Science and Technology, Department of Telecommunications, al. Mickiewicza 30, 30-056 Krakow, Poland
[2] Consorzio Interuniversitario Nazionale per l'Informatica, University of Naples Naples, Italy
{kkosek, natkaniec, vollero}@ieee.org

Abstract. The problem of content delivery with a required QoS is currently one of the most important. In ad-hoc networks it is IEEE 802.11 EDCA which tries to face this problem. This paper describes several EDCA line topology configurations with mixed priorities of nodes. Detailed conclusions about the innovative results help to understand the behavior of EDCA in the presence of hidden and exposed nodes. They reveal a strong unfairness in medium access between certain nodes dependent on their placement. They prove that for short lines a frequent inversion in the throughput levels of high and low priority traffic occurs and makes reliable content exchange impossible. The importance of the strength of the exposedness and hiddenness of nodes is also discussed. Furthermore, the usefulness of the four-way handshake mechanism is argued and descriptions of the known solutions to the hidden and exposed node problems are given. Finally, novel conclusions about EDCA are provided.

Keywords: EDCA, hidden and exposed nodes, QoS, simulations.

1 Introduction

License-free wireless LAN (WLAN) technologies allow wireless community networks to be created effortlessly. People can easily deploy WLANs to provide new services and exchange multimedia content from digital cameras, media centers, laptops, palmtops, mp3 recorders, mobile phones, camcorders, iPhones, etc. These new services include: streaming audio information like community radio, voice over IP (VoIP), video on demand (VoD), IP television (IPTv), online gaming using community game servers, neighborhood watch (providing surveillance, crime prevention and safety), p2p connections, shared Internet gateways and many others. In this article the authors focus on wireless ad-hoc networks which seem one of the most promising access technologies, and which will surely play an important role in

* This work has been realized under NoE CONTENT project no. 038423 within TA1 (Community Networks and Service Guarantees).

the nearest future. These networks without infrastructure will allow users fast and easy configuration of wireless networks anytime and anywhere. They will play the role of community networks which greatly facilitate the network forming process and provide Internet access for neighborhood groups, small businesses, towns, schools, organizations, companies, and many others. They will become irreplaceable during conferences, project meetings, gatherings and situations in which fast network deployment is a crucial factor.

Currently existing wireless networks have demonstrated that it is possible to efficiently deal with data services (e.g., Internet connectivity). Therefore, there is a growing expectation that these networks will efficiently deal with multimedia services as well. As an answer to the variety of the QoS (Quality of Service) requirements of different traffic types, the EDCA (Enhanced Distributed Channel Access) function was proposed [1]. However, the nature of ad-hoc networks makes the task of serving delay sensitive or bandwidth consuming traffic with a proper QoS very complicated. Therefore, it has been proven that EDCA tends to cease to function in imperfect conditions [10].

The two most troublesome characteristics of wireless networks are the following. Network users share a common radio channel, usually with limited access control, making traffic delivery fluctuant and unpredictable. Network capacity is also threatened by the problem of hidden and exposed nodes. The authors focus on the second issue, which they find more interesting.

The authors have found it crucial to check if current ad-hoc networks are able to provide QoS in the most typical topologies. This paper focuses on line topology scenarios. The purpose of analyzing line topology networks is very simple. A good example of such a topology is an ad-hoc network in which nodes communicate with a gateway every time they access Internet services. At the same time, most of these nodes are out of range of the gateway and need to send their data through their neighboring nodes. Other examples are long distance multihop links using the same radio channel which could be used in rural areas where access to the infrastructure part of a network is highly limited. The analysis of several basic line topology networks was described in [10]. Due to the unsatisfying results, it has encouraged the authors to analyze more complicated configurations, i.e., configurations with mixed priorities of nodes.

The analysis provided in this article helps to draw several novel conclusions about EDCA based ad-hoc networks. Among many consequences arising from the presence of hidden and exposed nodes within an ad-hoc network, the following seem the most important: (a) unfairness in granting medium access between different nodes, strongly dependent on their placement, (b) severely distorted order of the throughput levels of the access categories and frequent prioritizing of low priority traffic over high priority traffic, and (c) the inability of the four-way handshake mechanism to meaningfully improve the measured network performance.

The remainder of this paper is organized as follows. Section 2 contains the state-of-the-art in which the most important solutions of the hidden and exposed node problems and the EDCA function are described. Section 3 and Section 4 contain the simulation scenarios and simulation results, respectively. The concluding remarks are given in Section 5.

2 State-of-the-Art

In this section the following issues are briefly described: the EDCA function and the most important solutions of the hidden and exposed node problems. The description is aimed to organize the current knowledge about ad-hoc networks and their ability to satisfy the QoS requirements of different traffic classes. Additionally, the known flaws of the chief solutions of the hidden and exposed node problems are stressed in this section.

2.1 EDCA Function of the IEEE 802.11 Standard

The IEEE 802.11 standard defines two medium access functions with QoS support – EDCA (Enhanced Distributed Channel Access) and HCCA (Hybrid Coordination function Channel Access). EDCA is described in more details next because it was designed for the purpose of ad-hoc networks. For more details on HCCA, designed for infrastructure networks, see [1].

The EDCA mechanism defines several extensions to the traditional medium access procedure (Carrier Sense Multiple Access with Collision Avoidance) in order to assure the transportation of different traffic types with a proper QoS. It introduces four Access Categories (AC) differenced by their access parameters. They are Voice (VO), Video (VI), Best Effort (BE) and Background (BK). Since VO and VI are more jitter, delay and packet loss sensitive they have a higher priority than BE and BK.

Inside a QoS node each frame of a particular traffic stream is mapped into an appropriate AC and then it is buffered into an appropriate hardware queue (Figure 1).

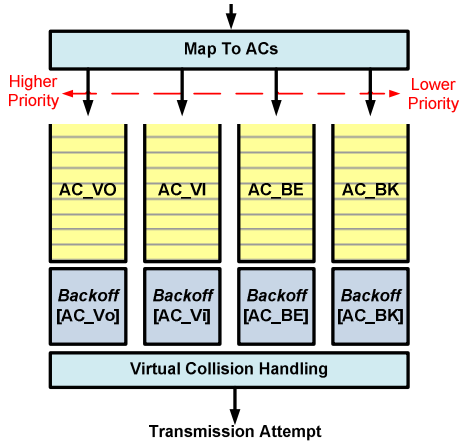


Fig. 1. Mapping into ACs [1].

For each frame the probability of being granted the channel access depends on the access parameters of the AC it belongs to. These parameters are Arbitration Inter-Fame Space Number — *AIFSN[AC]*, Contention Window minimum and maximum

boundary limits — *CWmin[AC]* and *CWmax[AC]*, and Transmission Opportunity Limit — *TXOPlimit[AC]*. The impact of these parameters on channel access prioritization is shown in Figure 2.

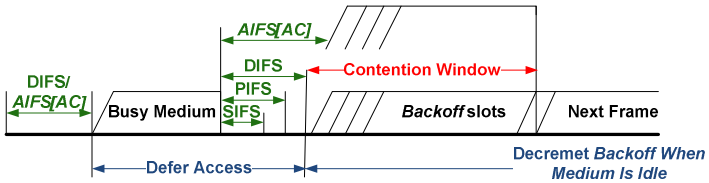


Fig. 2. Channel access prioritization [1].

The Backoff value is set to a random number from the number interval [0, *CW*]. Initially *CW* is set to *CWmin[AC]* but it increases (up to *CWmax[AC]*) whenever this AC is involved in a collision. *AIFS[AC]* is given by the following equation:

$$AIFSN[AC] = SIFS + AIFS[AC] \times SlotTime \quad (1)$$

Every QoS node is assigned the right to transmit after the medium was sensed idle for *AIFS[AC]* and when the Backoff time has elapsed. Therefore, the smaller the *AIFSN[AC]* and the *CW* sizes, the higher the probability of being granted access to the wireless medium before other ACs.

Two types of collisions may occur during the EDCA channel access procedure — virtual and physical. A virtual collision happens when more than one AC is granted the right to transmit at the same time. In such a case, a QoS node is obliged to send the higher priority frame and delay the lower priority ones. A physical collision occurs when two or more QoS nodes start their transmissions over the wireless medium simultaneously. The second type of collisions is common for hidden and exposed nodes.

2.2. Examples of Solutions of the Hidden and Exposed Node Problems

Solutions to the hidden and exposed node problems can be divided into the three groups: (a) sender-initiated, (b) receiver-initiated and (c) hybrid solutions.

The most known sender-initiated mechanism which minimizes the destructive effects of hidden nodes is the four-way handshake [1]. It uses four different types of frames: Request to Send (RTS), Clear to Send (CTS), Data (DATA) and Acknowledgement (ACK). Unfortunately, the four-way handshake mechanism has several disadvantages. Firstly, it is unable to eliminate the problem of hidden nodes when the network is multihop. Secondly, it cannot solve the problem of exposed nodes at all. Additionally, the four-way handshake consumes bandwidth even if no hidden nodes appear within the network. Furthermore, due to the exchange of additional signaling frames (i.e., RTS and CTS), the mechanism is unsuitable for delay sensitive traffic. An improvement to the four-way handshake is Multiple Access with Collision Avoidance for Wireless (MACAW, [4]) where five different types of frames are exchanged: RTS, CTS, Data Sending (DS), DATA and ACK. In order to

increase the per-node fairness MACAW involves an additional Request to RTS (RRTS) control frame. The biggest weakness of MACAW is the unsolved exposed node problem and furthermore, the increased signaling overhead. Another solution is the RTSS/CTSS mechanism [5]. This solution involves new types of RTS and CTS frames, namely RTS-Simultaneously and CTS-Simultaneously, in order to coordinate concurrent transmissions over exposed links. The main drawback of the RTSS/CTSS method is the requirement of modification in the PHY layer which prevents its implementation in currently available hardware.

The most known receiver-initiated protocol is Multiple Access Collision Avoidance By Invitation (MACA-BI, [6]) where a three-way handshake mechanism (CTS/DATA/ACK) is invoked for every frame transmission. However, the mechanism is suitable only for infrastructure networks. In ad-hoc networks polling a node without packets to be sent is a waste of time.

Hybrid solutions, e.g. [7], are built on the basis of both the sender- and receiver-initiated mechanisms. Their main aim is to combine the advantages and eliminate the main weaknesses of the previous solutions. These mechanisms assure better fairness and decrease end-to-end delay. However, they cannot guarantee QoS for delay sensitive traffic and were tested only in pure DCF environments.

Apart from the mentioned protocols, there exists a family of mechanisms which involve busy tone signals in order to combat the hidden and/or exposed node problems. The most known solution is Dual Busy Tone Multiple Access (DBTMA, [8]). DBMA uses two busy tone signals and two sub-channels to avoid hidden and exposed nodes. However, it does not take into account the possible interference on the control channel and does not involve ACKs. Resigning from ACKs seems illogical in the case of the unreliable wireless channel. Another solution is Floor Acquisition Multiple Access with Non-persistent Carrier Sensing (FAMA-NCS, [9]). It takes advantage of using long CTS frames, which aim to prevent any contending transmissions within the receiver range. Unfortunately, this scheme requires all nodes to hear the interference which makes the mechanism inefficient in case of short DATA frames.

To the authors' best knowledge, a good solution of the hidden and exposed node problems for EDCA based networks does not exist. Most of the current solutions are mainly based on the four-way handshake mechanism or mechanisms similar to it (e.g., [11]-[14]).

To summarize, even though there are several concurrent solutions to the four-way handshake mechanism in the literature, none of them have become popular enough to be broadly used. Additionally, in order to deal with the hidden node problem, the IEEE 802.11 standard suggests the use of the four-way handshake method and does not recommend any protocol to deal with the exposed node problem. Therefore, as the best candidate, only this protocol is analyzed during the conducted tests.

3 Simulation Scenarios

The simulation analysis was performed with the use of an improved version of the TKN EDCA implementation [2] for the ns2 simulator. The adjustments made mostly

affect, but are not limited to, the four-way handshake mechanism which was not supported by the original version of the TKN EDCA patch and the process of handling duplicate frames. All important simulation parameters are given in Table 1 and Table 2.

Table 1. EDCA parameter set [1].

Access Category	CWmin[AC]	CWmax[AC]	AIFSN[AC]	TXOP
VO	7	15	2	0
VI	15	31	2	0
BE	31	1023	3	0
BK	31	1023	7	0

Table 2. General simulation parameters.

SIFS	10 µs	**DIFS**	50 µs
IFQ length	5000 frames	**Slot Time**	20 µs
Tx Range	250 m	**Tx Power**	0.282 W
Frame Size	1000 B	**Traffic Type**	CBR/UDP
CS Range	263 m	**Node Distance**	200 m

The authors assumed that all nodes send CBR traffic with a varying sending rate. DSSS is used at the PHY layer and the EDCA function is set as the MAC layer type. In all configurations, nodes form line topology networks in which each node can only detect the transmissions of its nearest neighbors. The number of nodes changes from 3 to 5 depending on the configuration (see Figure 3). The analysis is performed on a single-hop basis because the authors focus only on the MAC layer. IP layer connections are out of the scope of this paper.

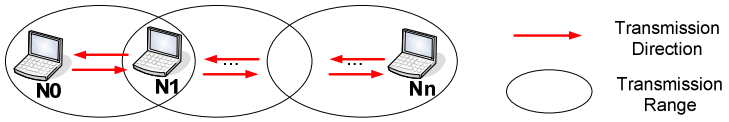


Fig. 3. Simulated networks.

The main aim of the performed tests lies in showing how serious is the impact of hidden and exposed nodes on EDCA performance and, furthermore, how much it depends on the configured priorities. In all simulations the packet generation times of different nodes are not synchronized and a frame size of 1000 B is assumed for all traffic priorities. This assumption is made, primarily, in order to compare the four EDCA queues under similar conditions and, secondly, to avoid ineffective transmissions of small DATA frames. For all configurations two cases are analyzed: basic channel access (DATA/ACK) and the four-way handshake mechanism

(RTS/CTS/DATA/ACK). Furthermore, configurations with only VO and BK priorities of nodes are tested because their performance is very similar to that of VI and BE, respectively [10]. In all figures the error of each simulation point for a 95 % confidence interval does not exceed ± 2 %.

4 Simulation Results

Several different configurations of line topology scenarios with mixed priorities were analyzed. The most interesting ones are given in Table 3. In all configurations the carrier sensing range for all nodes was set to 263 m in order to achieve hidden and exposed nodes within a network (c.f., Figure 3 and Table 2 in which node distance equals 200 m).

Table 3. Configurations of line topology networks with mixed priorities.

Network	**Three-node line**			**Four-node line**		**Five-node line**		
Configuration No.	**1**	**2**	**3**	**1**	**2**	**1**	**2**	**3**
N0	VO	VO	BK	VO	BK	BK	BK	VO
N1	BK	VO	BK	BK	VO	BK	VO	BK
N2	VO	BK	VO	BK	VO	VO	BK	BK
N3	-	-	-	VO	BK	BK	VO	BK
N4	-	-	-	-	-	BK	BK	VO

To simplify understanding of the behavior of nodes, the authors present the throughput values obtained by different nodes (under every network load) and frame loss (under maximum network load) for all configurations. The following types of frame losses are taken into account:

- **Duplicate (DUP) drops**– the result of collisions of either DATA and ACK frames or RTS and ACK frames caused mainly by the exposedness of nodes. The collision on an ACK frame causes a retransmission of the corresponding DATA frame. As a result, the node which previously sent the ACK receives the same DATA frame and drops it.
- **Collisions (COL)** – occur when DATA frames are lost due to a collision.
- **Retransmission (RET) drops** – occur when frames are dropped due to the transgression of the short or long retransmission limits.
- **IFQ drops** – frames dropped in the MAC queues.
- **ARP drops** – the result of not receiving ARP replies.

The authors put a stress on the most important losses in each analyzed configuration in order to clearly explain the figures representing throughput. All presented values are normalized per-node and per-collision domain in order to simplify the comparison of nodes from different collision domains.

4.1 Three-node Network

According to the IEEE 802.11 standard, the higher the priority the more often nodes may compete for medium access. As a result, in the case of a three node line network (Figures 4-6), the hidden nodes (N0 and N2) experience a higher number of collisions when their priority is higher. In the case of this network the RTS/CTS mechanism eliminates the problem of DATA collisions. Therefore, if it is enabled the number of COLs counted for the hidden nodes decreases practically to zero. As a consequence, N1 does not have to wait long for its data transmission and has more chances to send its traffic (Figure 4). At the same time, the throughput achieved by the hidden nodes is unsatisfactorily low. This is because of permanent collisions of RTS frames sent by these nodes.

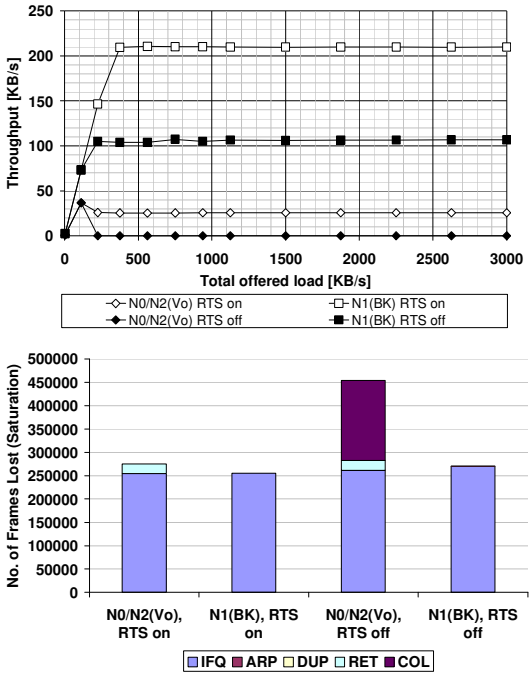
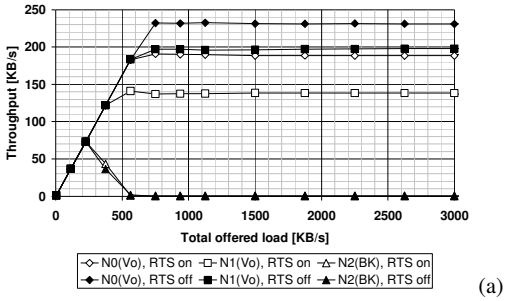
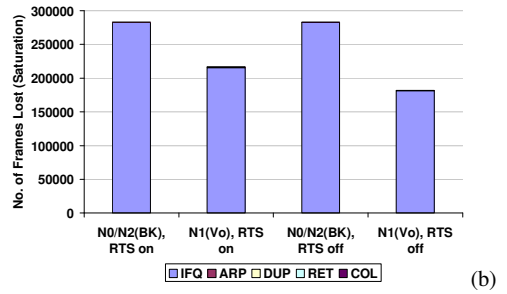


Fig. 4. 3-node line: throughput (a) and frame losses (b) in Configuration 1.

Additionally, comparing Configurations 1-3, it can be seen that the synchronization of hidden nodes sending high priority traffic is the most severe problem for Configuration 1. This synchronization is a result of the fact that 1000 B frames need more than 36 time slots (for DSSS) for an uninterrupted transmission. Unfortunately, for VO the value of CWmax is equal to 15 and, therefore, the unacceptable number of collisions, causing a severe reduction of throughput, is unavoidable (Figure 4).

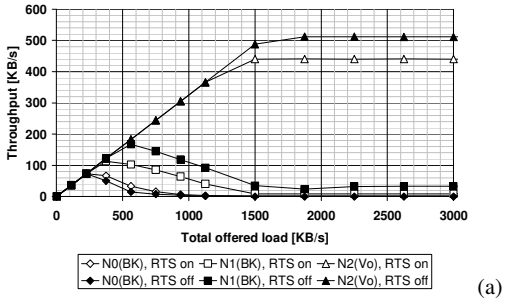


(a)

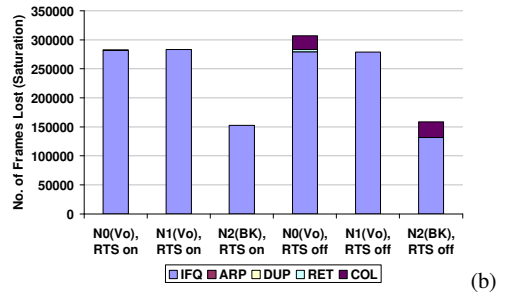


(b)

Fig. 5. 3-node line: throughput (a) and frame losses (b) in Configuration 2.



(a)



(b)

Fig. 6. 3-node line: throughput (a) and frame losses (b) in Configuration 3.

Furthermore, the priority of the unhidden node N1 influences the throughput values of the hidden nodes. However, this is not the main cause of the problems with serving high priority streams by EDCA. In Figure 5 it is shown, that the high priority of N1 does not completely degrade the performance of the hidden node with the high priority traffic. On the other hand, Figure 6 shows that the unhidden N1 may be favored over the hidden N0 when they transmit traffic of the same priority. Furthermore, it appears that enabling RTS/CTS is not always reasonable because it may decrease the throughput values (Figure 5 and Figure 6).

4.2 Four-node Network

In the four-node line scenario enabling RTS/CTS degrades its performance (Figures 7-8). This happens especially when the middle nodes transmit high priority traffic (Figure 8). This behavior can be explained by the high number of RET drops and, furthermore, by the increased signaling overhead.

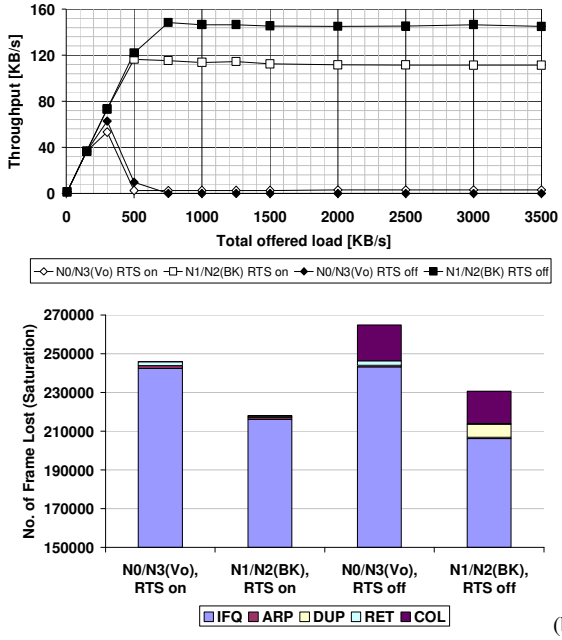


Fig. 7. 4-node line: throughput (a) and frame losses (b) in Configuration 1.

It is interesting that in Configuration 1 (Figure 7) the exposed nature of the middle nodes plays the most important role (i.e., they experience a lot of DUP drops) and in Configuration 2 (Figure 8) their hidden nature (i.e., they do not experience many DUP drops) is influenced. The main reason is that in Configuration 1 the side nodes send VO (causing multiple collisions on ACK frames from either N1 or N2 as well as ARP

drops) and in Configuration 2 the middle nodes send VO (causing mostly collisions on either frames from N0, N3 or from themselves). In both cases nodes sending VO traffic have a significant number of IFQ drops because after each COL they have to resend the collided DATA frame and cause meaningful delays in sending new DATA frames. Therefore, also with RTS/CTS disabled, nodes with low priority traffic win medium access most often.

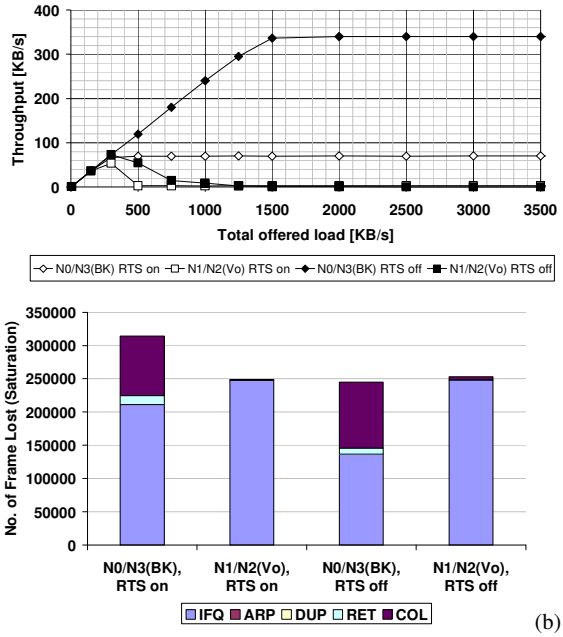


Fig. 8. 4-node line: throughput (a) and frame losses (b) in Configuration 2.

4.3 Five-node Network

The performance of the five-node line appeared similar to the performance of the six- and the seven-node line (c.f., [10]), therefore, the authors decided to test only this network with mixed traffic priorities. The most interesting conclusion from the analysis of this network is that in general high priority traffic is favored over low priority traffic regardless of the position of the transmitting nodes (Figures 9-11). Obviously, a similar behavior is expected for the six- and the seven-node networks.

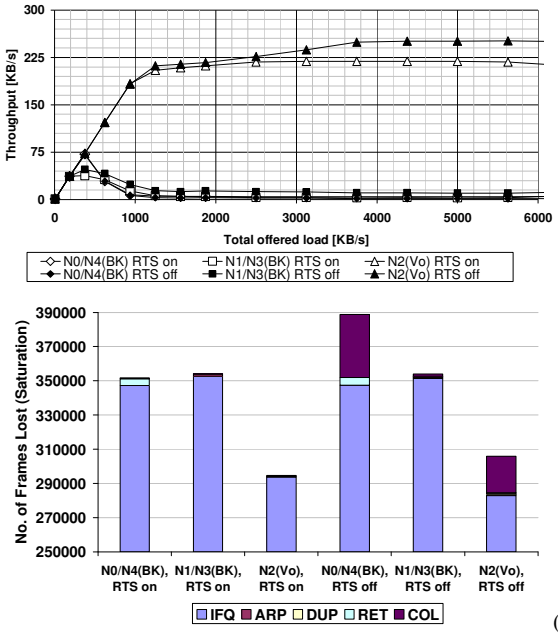
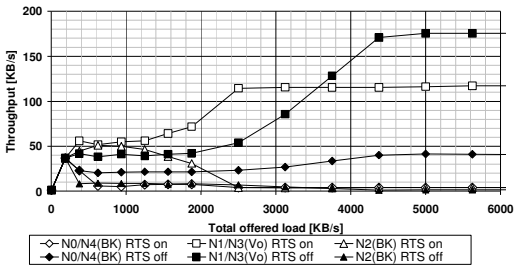
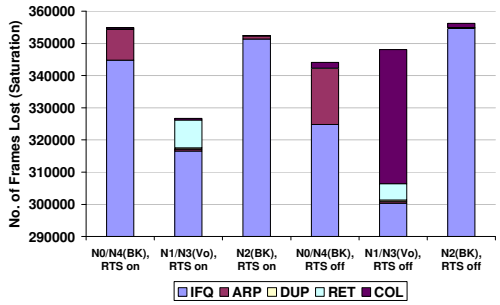


Fig. 9. 5-node line: throughput (a) and frame losses (b) in Configuration 1.

In Configuration 1 (Figure 9) the network performance is self-explainable. The middle node is the only one with the high priority. It collides mostly with the side nodes sending low priority traffic which do not win medium access very often. In Configuration 3 (Figure 11) the situation is again very simple. This time only the side nodes have high priority and, as a result, may send their traffic most often. They collide mostly with the middle node, which sends low priority traffic. The most interesting is Configuration 2 (Figure 10) in which N1 and N3 (sending VO) can collide with any node. Additionally, due to their placement, they experience some DUP drops. Under a small network load, the number of DUP drops as well as the number of RET drops is the highest for N1 and N3, however, the number of IFQ drops is the smallest. As a result, their throughput is visibly limited. As the network load grows, also the throughput of N1 and N3 increases. This performance can be explained by the strong hiddenness of the middle node N2. This node experiences the highest number of IFQ drops under practically every network load. However, with the increase of the offered load its inferiority becomes even more evident. Obviously, nodes sending the same priority traffic do not achieve the same throughput. This observation leads to a conclusion that also in this configuration the problem of unfairness between certain nodes appears and it depends on the nodes' positions. Additionally, similarly to the four-node line, in all analyzed configurations enabling RTS/CTS decreased the obtained throughput values.

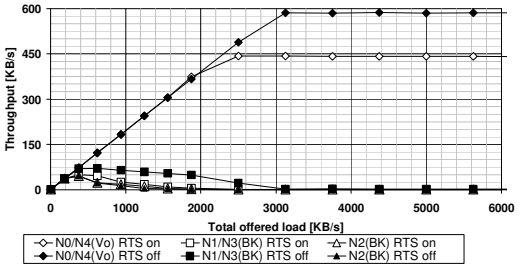


(a)

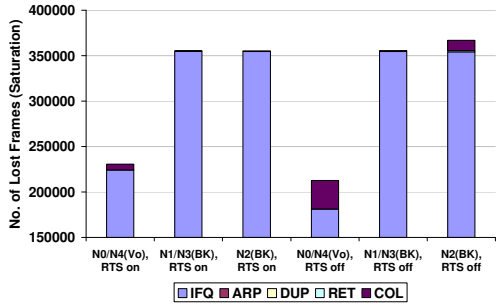


(b)

Fig. 10. 5-node line: throughput (a) and frame losses (b) in Configuration 2.



(a)



(b)

Fig. 11. 5-node line: throughput (a) and frame losses (b) in Configuration 3.

5 General Conclusions

This paper presents a novel simulation study of line topology ad-hoc networks based on EDCA in which nodes are assigned different priorities. The problems caused by the hiddenness and exposedness of nodes are commented in details. Most of all, it is noticed that the analyzed networks are unable to transport high priority traffic with a desired QoS. Moreover, the paper argues the usefulness of the use of the RTS/CTS mechanism which, in most cases, does not improve the performance of the simulated networks but rather causes a decrease of the obtained throughput values.

The most important conclusions are the following. When we look at the three-node line network, the problem of synchronization of hidden nodes is the most severe one. Especially with RTS/CTS disabled, it causes a strong reduction of the throughput values of the high priority streams. The priority of the middle node is also crucial because it influences the values of the throughput levels of the neighboring nodes, however, it is not the main reason of the inability in providing their streams with a desired QoS. The performance of the four-node line topology is the most unpredictable because nodes which were previously prioritized are no longer superior. This can be explained by either the strong hiddenness or exposedness of the middle nodes, depending on the actual network configuration. The performance of longer line topologies is much better. In all analyzed cases, nodes sending high priority traffic were favored over nodes sending low priority traffic. Therefore, their performance was close to that which is required by the IEEE 802.11 standard. Unfortunately, the unfairness in granting medium access between nodes sending traffic of the same priority was also revealed.

On the basis of all observations, the authors find dealing with line topology networks with mixed priority traffic as the most troublesome when the lines are short. However, from a wider perspective, the performance of all measured networks is completely unacceptable. Every simulation scenario disclosed a severe unfairness in granting medium access between certain nodes. Therefore, the authors find it crucial to find a novel mechanism which will improve the fairness between nodes and make the traffic delivery reliable even if hidden or exposed nodes are present within a network. In particular, they think that the awareness of nodes should increase. For this reason, their future research will be focused on defining new metrics, which should be taken into account during the design of a new MAC protocol.

References

1. "IEEE 802.11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Inc., (2007).
2. TKN EDCA 802.11e extension. http://www.tkn.tuberlin.de/research/802.11e_ns2, (2006).
3. Bai, X., Mao, Y. M.: The Impact of Hidden Nodes on MAC Layer Performance of Multi-hop Wireless Networks Using IEEE802.11e Protocol. International Conference on Wireless Communications, Networking and Mobile Computting, WiCom 2007, (2007)
4. Bharghavan, V., Demers, A., Shenker, S., Zhang, L.: MACAW: A Media Access Protocol for Wireless LAN's. ACM SIGCOMM 1994, (1994)

5. Mittal, K., Belding, E.M.: RTSS/CTSS: Mitigation of Exposed Terminals in Static 802.11-based Mesh Networks. The 2nd IEEE Workshop on Wireless Mesh Networks, WiMesh 2006, (2006)
6. Talucci, F., Gerla, M., Fratta, L.: MACA-BI (MACA by invitation) - A Receiver Oriented Access Protocol for Wireless Multihop Networks. The 8th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, IEEE PIMRC 1997, (1997)
7. Wang, Y., Garcia-Luna-Aceves, J.J.: A New Hybrid Channel Access Scheme for Ad Hoc Networks. The 1st IFIP Annual Mediterranean Ad Hoc Networking Workshop, MedHocNet 2002, (2002)
8. Haas, Z.J., Deng, J.: Dual Busy Tone Multiple Access (DBTMA) – A Multiple Access Control for Ad Hoc Networks. IEEE Transactions on Communications, (2002)
9. Fullmer, C.L., Garcia-Luna-Aceves, J.J:. Solutions to Hidden Terminal Problems in Wireless Networks, ACM SIGCOMM 1997, (1997)
10. Kosek, K., Natkaniec, M., Pach, A.R.: Analysis of IEEE 802.11e Line Topology Scenarios in the Presence of Hidden Nodes. The 7th International Conference on AD-HOC Networks & Wireless, AdHoc-NOW 2008, (2008)
11. Hamidian, A., Körner, U.: Providing QoS in Ad Hoc Networks with Distributed Resource Reservation. 20th International Teletraffic Congress, ITC 2007, (2007).
12. Ying, Z., Ananda, A.L., Jacob, L.: A QoS Enabled MAC Protocol for Multi-hop Ad Hoc Wireless Networks. The 22nd IEEE International Performance, Computing, and Communications Conference, IPCCC 2003, (2003)
13. Benveniste, M., Tao, Z.: Performance Evaluation of a Medium Access Control Protocol for IEEE 802.11s Mesh Networks. IEEE Sarnoff Symposium, (2006)
14. Choi, S. Kim, S., Lee, S.: The Impact of IEEE 802.11 MAC Strategies on Multi-hop Wireless Mesh Networks. The 2nd IEEE Workshop on Wireless Mesh Networks, WiMesh 2006, (2006)