Analysis of IEEE 802.11e Line Topology Scenarios in the Presence of Hidden Nodes

Katarzyna Kosek, Marek Natkaniec, Andrzej R. Pach

AGH University of Science and Technology, Krakow, Poland
{kosek, natkanie, pach}@kt.agh.edu.pl
http://www.kt.agh.edu.pl/

Abstract. In this paper an innovative simulation study of five IEEE 802.11e network configurations is presented. The conducted analysis is crucial for understanding how a theoretically simple and, most of all, popular line topology network can be degraded by the presence of hidden and exposed nodes. The discussion of the obtained results helps to understand how and why the behavior of IEEE 802.11e based line topologies changes when the number of nodes increases. Furthermore, the usefulness of the four-way handshake mechanism is argued and brief descriptions of the most known solutions of the hidden and exposed node problems are given. Finally, the need for a better MAC protocol is stressed and a number of novel conclusions about the IEEE 802.11e nature is provided.

Key words: ad-hoc, hidden and exposed nodes, IEEE 802.11e

1 Introduction

Wireless networking technology is quickly evolving and its importance grows constantly. The most interesting technology, not only from the perspective of a researcher but also from the perspective of an average user, seem to be ad-hoc networking. These networks without infrastructure do not need complicated administration and may greatly facilitate Internet access. Unluckily, all wireless networks were created to deal with data exchanges and not multimedia services. Therefore, the need for QoS assurance for delay sensitive and/or bandwidth consuming services remains an interesting and unresolved issue. Constantly changing and unpredictable channel conditions, hidden and exposed node problems, varying network load, changeable device performance, different transmission and sensing ranges, and mobility of ad-hoc networks make it an even more difficult task. In this article the authors focus on the hidden and exposed node problems which they find the most interesting.

Five different configurations of ad-hoc line topologies are simulated. The purpose of analyzing line topologies is simple. A good example of such a case in a real environment is a simple mesh network in which ad-hoc nodes communicate with a gateway (GW) every time they access the Internet services. At the same time, most of these nodes are out of range of GW and need to send their data through other nodes. Another example are long distance multi-hop links using the same radio channel which could be used in rural areas where access to infrastructure is highly limited.

Due to the fact that all kinds of topologies require QoS, the authors found it crucial to check if IEEE 802.11e can assure QoS guarantees in such environments. This paper presents novel results regarding line topologies. To the authors' best knowledge similar analysis has not been performed. Related work can be found in [4] in which, however, the authors did not take into account different line topologies and did not analyze how the length of a line impacts the network performance. Additionally, they did not notice the undesirable inversion in prioritizing traffic and, furthermore, the values of EDCA access parameters used were not compatible with the IEEE 802.11e standard.

The analysis presented in this article helps to draw innovative conclusions about IEEE 802.11e behavior. Among many consequences of the hidden and exposed nodes presence, the most important seem the unavoidable unfairness in granting medium access and distortion of the throughput levels of different priority streams. The paper also gives a brief description of the known solutions of the hidden and exposed node problems and argues the usefulness of the four-way handshake method in minimizing their degrading impact on IEEE 802.11e performance. Additionally, the gathered results are compared with the results obtained for two different star topology networks presented in [5].

The remainder of this paper is organized as follows. Section 2 contains the state-of-the-art. In Section 3 the description of the simulation scenarios can be found. Section 4 gives explanation of the obtained results and presents scrupulous conclusions. More general conclusions can be found in Section 5.

2 State-of-the-Art

2.1. Hidden and Exposed Node Problem

WLAN terminals work in a half-duplex mode, thus they cannot transmit while receiving data. The result of such operation is that the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) procedure cannot detect hidden and exposed nodes. Such nodes cause interference and unnecessary delay and, therefore, the whole network performance is degraded.

In Fig. 1, nodes A and C are hidden from each other, likewise nodes B and D. Additionally, nodes B and C are exposed. Let us imagine two situations. In the first one, nodes A and C try to transmit their data to B at exactly the same time. In the second one, while node B transmits its data to node A, node C would like to start its transmission to D. In the first situation, both transmissions will fail. In the second one, node C will not be able to transmit due to B's transmission, even though node D is out of the range of B. It must be stressed that these types of situations are frequent and, especially in multi-hop environments (i.e., ad hoc or mesh networks), they are severe problems.

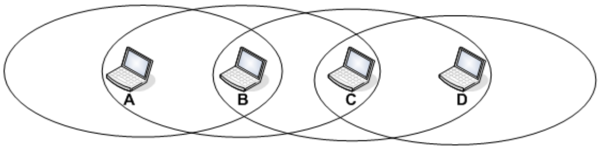

Fig. 1. Hidden and exposed nodes

2.2. Solutions to the Hidden and Exposed Node Problems

The most known sender-initiated solution minimizing the destructive effects of the hidden nodes is the four-way handshake. The mechanism uses four different types of frames, i.e., Request to Send (RTS), Clear to Send (CTS), Data (DATA) and Acknowledgement (ACK). These frames are exchanged during the process of granting the medium access. Unfortunately, the four-way handshake has several disadvantages. Firstly, it is optional in the IEEE 802.11 standard. Secondly, this method is unable to eliminate the problem of hidden nodes when the network is multiple-hop. Thirdly, this mechanism consumes bandwidth even if no hidden nodes appear within the network. Furthermore, due to the exchange of the additional RTS/CTS frames, the mechanism is unsuitable for delay-sensitive traffic. An important improvement to the four-way handshake is Multiple Access with Collision Avoidance for Wireless (MACAW, [6]) where five different types of frames are exchanged, i.e., RTS, CTS, Data Sending (DS), DATA and ACK. In order to increase the per-node fairness MACAW involves a Request to RTS (RRTS) control frame. The biggest weakness of MACAW is the unsolved exposed node problem and furthermore, the increased signaling overhead. One other solution is the RTSS/CTSS mechanism [12]. 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. This helps to mitigate the problem of exposed nodes. The biggest disadvantage of the RTSS/CTSS method is the requirement of modification in the PHY layer which makes its implementation on the currently available hardware impossible.

The most known receiver-initiated protocol is Multiple Access Collision Avoidance By Invitation (MACA-BI, [7]) where a three-way handshake mechanism (CTS/DATA/ACK) is invoked for every frame transmission. However, this mechanism is suitable rather for infrastructure than for ad-hoc networks. In ad-hoc networks polling a station without packets to be sent is a waste of time.

On the basis of the sender- and receiver-initiated mechanisms, due to their weaknesses, hybrid solutions were proposed (e.g., [8]). 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 IEEE 802.11 environments.

There also exists a family of protocols involving busy tone signals in order to combat problems caused by hidden and/or exposed nodes. The most known solutions are Busy Tone Multiple Access (BTMA, [9]) and Dual Busy Tone Multiple Access

(DBTMA, [10]). BTMA is dedicated for infrastructure networks. DBMA uses two busy tone signals and two sub-channels to avoid hidden and exposed nodes. However, it does not pay attention to 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. One other solution is Floor Acquisition Multiple Access with Non-persistent Carrier Sensing (FAMA-NCS, [11]). It takes advantage of using long CTS frames which aim to prevent any contending transmissions within the receiver's range. Unfortunately, this scheme requires all nodes to hear the interference which makes the mechanism inefficient in case of short DATA frames.

As it was shown, there are several concurrent solutions to the four-way handshake mechanism in the literature, however, none of them have become popular enough to be broadly used. Additionally, also the IEEE 802.11 standard suggests the use of the four-way handshake method to deal with the hidden node problem and does not recommend any protocol as a remedy to the exposed node problem. Therefore, only this protocol is validated during the performed tests.

3 Simulated Scenarios

The simulation analysis was performed with the use of an improved version of the TKN EDCA enhancement [3] to the ns2 simulator. The adjustments made mostly affect the RTS/CTS mechanism which was not supported properly by the original version of the TKN EDCA patch. Additionally, the handling of duplicate drops was fixed. Important simulation parameters are given in Table 1 and Table 2.

Table 1. EDCA parameter set

Priority	AC	*$CW_{min}[AC]$*	*$CW_{max}[AC]$*	*AIFSN[AC]*	*TXOP*
P0	Vo	7	15	2	0
P1	Vi	15	31	2	0
P2	BE	31	1023	3	0
P3	BK	31	1023	7	0

Table 2. General simulation parameters

SIFS	10 µs	***DIFS***	50 µs
PIFS	30 µs	***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 simulation study was performed with the assumptions that all nodes send CBR traffic with a varying sending rate (from 10 kb/s to 10 Mb/s) and the IEEE 802.11b standard is used as the physical layer type. The nodes form line topologies in which each node can only detect transmissions of its nearest neighbors (c.f., Fig. 11). The number of nodes changes from 3 (numbered from left to right N0-N2) to 7 (N0-N6).

Additionally, for every analyzed network setup, four different EDCA configurations are simulated. In each configuration a different EDCA class is used for the flows generated by the network-forming nodes.

In order to combat the hidden node problem the RTS/CTS mechanism is used. Additionally, for the sake of clarity of the presented figures, if two nodes obtain similar throughput it is presented as a single mean value (e.g., N0/N2 for nodes N0 and N2 in Fig. 2). For the same reason, in Fig. 3-Fig. 5 only the curves representing Vo and BE priority are presented because their performance is very similar to that of Vi and BK, respectively (c.f., Fig. 3). Moreover, in all presented figures the error of each simulation point for a 95 % confidence intervals does not exceed ± 2 %.

4 Simulation Results

In this section the results obtained for the three- to seven-node line scenarios will be described. Firstly, the overall performance of particular networks will be analyzed by comparing the obtained throughput by nodes for four different priorities. Secondly, the six-node line will be described in detail by means of frame dropping probability, retransmission drops and duplicate drops. Finally, a comparison with two star topology networks ([5]) will also be given.

4.1. Three-node Line

With the RTS/CTS exchange disabled, hidden nodes with Vo and Vi priorities obtain smaller throughput than BE and BK in general (Fig. 2a). Furthermore, when the overall traffic load exceeds 225 KB/s, the throughput of Vi and Vo streams drops to zero. For the unhidden node, the order of the throughput levels is in line with the IEEE 802.11e guidelines.

With RTS/CTS enabled, the throughput of hidden nodes slightly increases and drops for the unhidden node (Fig. 2b). However, the strong unfairness between the hidden and unhidden nodes is not eliminated. Additionally, when hidden nodes are transmitting Vo traffic the unfairness is strongest as they obtain the lowest throughput which is practically equal to zero for traffic load exceeding 500 KB/s.

The above observations lead to a conclusion that with RTS/CTS both enabled and disabled, the three-node line topology network will not work properly. In such a network, for hidden nodes, low priority traffic will be always prioritized over high priority traffic and, additionally, the unhidden node will be strongly prioritized over the hidden ones.

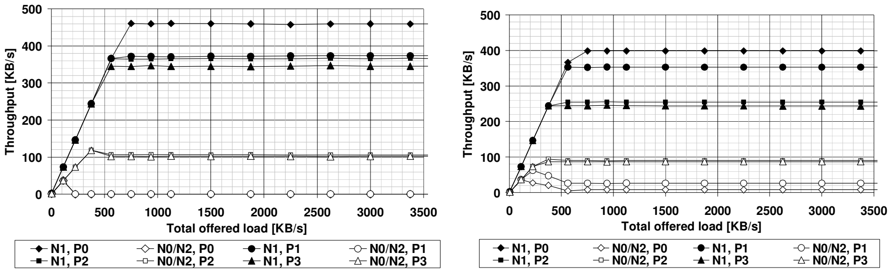

Fig. 2. Three-node line. Throughput for RTS/CTS (a) disabled (b) enabled.

4.2. Four-node Line

For a four-node line topology the throughput curves change (Fig. 3a) in comparison to the three-node line. With the RTS/CTS exchange disabled the throughput order may be divided into two main sets. Under lighter load (below 2 MB/s), N0/N3 transmitting BE and BK obtain higher throughput than N2/N4 transmitting Vi and Vo. Under heavier load, this order changes so the unfairness between these pairs of nodes is even stronger. Furthermore, under network load exceeding 150 KB/s, for all nodes, BE and BK priority streams are favored over Vi and Vo.

With RTS/CTS enabled, N1/N2 are prioritized over N0/N3 (Fig. 3b). Moreover, for all nodes low priority streams obtain higher throughput than high priority streams. In comparison to the three-node topology, the overall throughput drops and, therefore, the network performance of four-node line topology is worse for both enabled and disabled RTS/CTS.

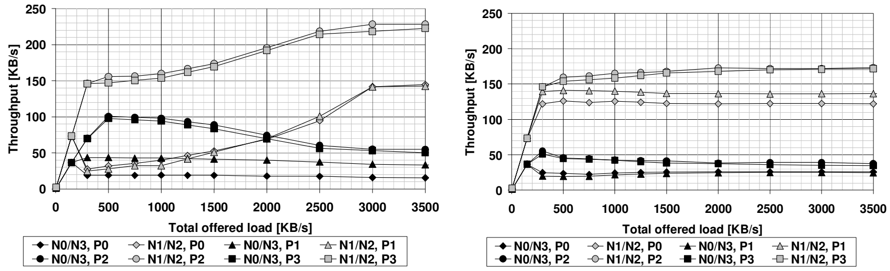

Fig. 3. Four-node line. Throughput for RTS/CTS (a) disabled (b) enabled.

4.3. Five-node Line

For the five-node line, with the RTS/CTS exchange disabled, for Vo priority traffic nodes N1/N3 obtain the highest throughput, N0/N4 smaller and N2 the smallest (which is totally unacceptable for network load over 375 KB/s). Moreover, the observed unfairness between certain nodes increases as the total offered load grows. For BE priority the order of N1/N3 and N0/N4 is reversed (Fig. 4a).

With the RTS/CTS exchange enabled, the throughput level order may be divided into two sets (Fig. 4b). The throughput levels under non-saturation conditions for N1/N3 and N0/N4 for Vo are the lowest but they grow with the increase of the offered load. Similarly, also the throughput of N0/N1/N3/N4 sending BE grows linearly. At the same time, a decrease in the throughput value of N2 can be observed for both BE and Vo. Finally, under network load of over 2.5 MB/s the throughput values are stable and N2 obtains smallest throughput regardless of the traffic priority it transmits. In all analyzed cases, BE is prioritized over Vo but the strongest unfairness is present for nodes N0 and N4.

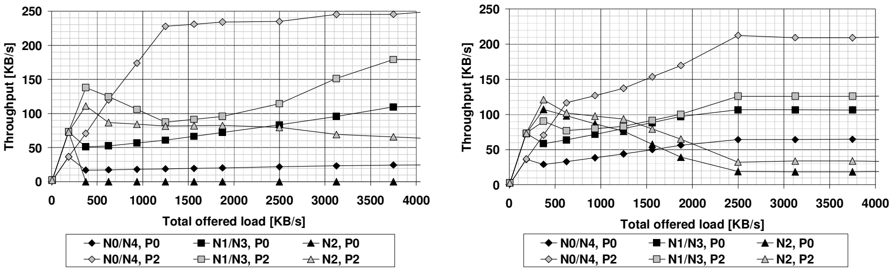

Fig. 4. Five-node line. Throughput for RTS/CTS (a) disabled (b) enabled.

4.4. Six-node Line

In case of the six-node line topology, the obtained results resemble the results for the four-node line in the case of Vo/Vi priority transmission. Which means that the nodes being in the middle of the line have the smallest throughput, the ones next to them win the competition for medium access most often and, finally, all other nodes receive average priority in medium access. However, in this configuration the unfairness between high priority traffic and low priority traffic is stronger because practically under every network load for RTS/CTS both enabled and disabled, all nodes sending Vo obtain smaller throughput than the corresponding ones sending BE (Fig. 5). The strongest unfairness is observed for the side nodes — N0/N5 (similarly to the four-node line's N0/N4) but it also increases for the nodes N1/N3.

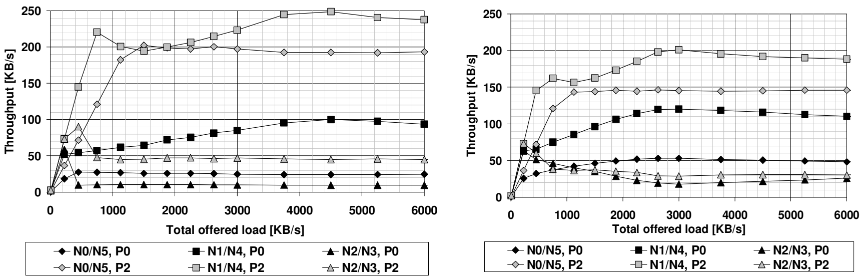

Fig. 5. Six-node line. Throughput for RTS/CTS (a) disabled (b) enabled.

4.5. Seven-node Line

The observations for the seven-node line are similar to the ones made for the six-node line. Once again, regardless of the RTS/CTS exchange, nodes sending high priority traffic streams obtain smaller throughput than the corresponding ones sending low priority streams. Additionally, N1/N5 win the competition for medium access most often, and the one in the middle (N3) less often. The main difference is that the strongest unfairness can be observed for nodes N1/N5 and not the side-nodes.

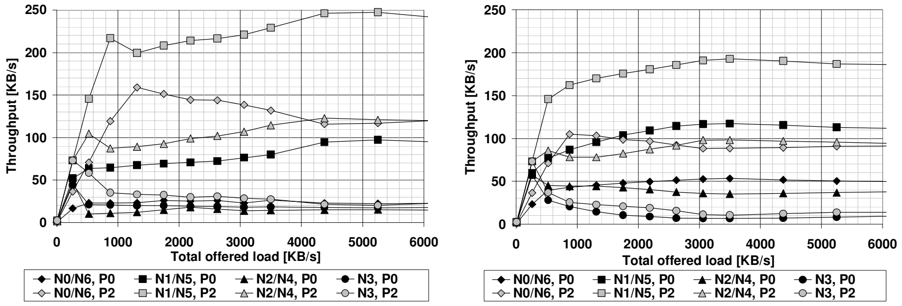

Fig. 6. Seven-node line. Throughput for RTS/CTS (a) disabled (b) enabled.

4.6. Overall Throughput

The overall saturation throughput levels obtained for the analyzed scenarios are presented in Fig. 7. As can be seen, for the high priority traffic the saturation throughput is highest for the shortest line. For the low priority traffic the situation changes because the saturation throughput grows meaningfully as the number of nodes increases. Additionally, in all cases the throughput of high priority traffic is smaller than for low priority traffic which differs from IEEE 802.11e assumptions.

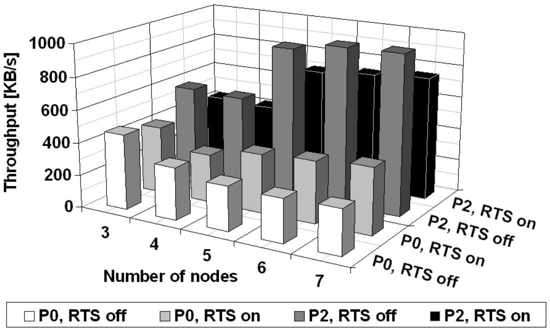

Fig. 7 Overall saturation throughput.

4.7. Detailed Conclusions

The performance shown in Fig. 2-Fig. 6 can be explained by the rate of the total frame loss for each of the analyzed flows in every simulation scenario. Additionally it can be also justified by the general character of each of the analyzed networks. For example in the case of the three-node line topology, two hidden and zero exposed nodes appear. In the five-node line there are five hidden nodes and three exposed ones, however, the hiddenness and exposedness of particular nodes differs.

Due to the lack of space only the performance of the six-node network will be explained in great detail with the help of the results presented in Fig. 8-Fig. 11. This network has been chosen as the most general one. The conclusions regarding this network will also be valid for the remaining ones.

The frame dropping probability is computed on the basis of the number of dropped frames in interface queues between the LLC and the MAC layers. In particular, it is the number of dropped frames to the number of generated frames.

$$P_{drop} = \frac{n_{dropped}}{n_{generated}} \,. \tag{1}$$

For RTS/CTS disabled (Fig. 8a), N2/N3 almost always have the same frame dropping probability. However, there is a great difference for N1/N4 and N0/N5 between Vo and BE. This behavior means that for BE the dropping probability is, in general, smaller than for Vo which differs from IEEE 802.11e assumptions. The dropping probability for N0/N5 is non zero for BE for the total offered load exceeding 1 MB/s, for Vo – exceeding 0.45 MB/s. In both cases, for all remaining nodes it starts earlier. Such a behavior could lead to an assumption that N0 and N5 should achieve highest throughput for both Vo and BE. When we look, however, at Fig. 5a and Fig. 5b, we see that these are N1 and N4 which outperform all other nodes. This is a result of the fact of the exposedness of N1 and N4 which leads to high number of duplicate drops (c.f., Fig. 11) described later in this section. In general, for BE non zero frame dropping probability starts later than for Vo which contradicts IEEE 802.11e. It is a result of less frequent attempts in obtaining medium access by BE. Higher priority means smaller values of EDCA access parameters and a higher possibility for competing for medium access. Such a behavior causes a higher probability of collisions for hidden nodes and, consequently, it leads to a higher number of retransmissions which cause quicker filling of the four MAC priority queues. As a result, the quicker a certain queue is filled the higher the probability that it will be overloaded and more interface queue drops will be observed. Obviously, the more duplicate frames are sent the higher probability that they will collide in the wireless medium instead of the good frames. Therefore, duplicate drops and retransmission drops should be analyzed together in order to understand this complicated behavior. One other thing which matters in analyzing the frame dropping probability curves is the type of their slopes. The steepness of slopes show how high is the speed of filling the MAC priority queues. Curve slopes are gentlest for N0/N5 and steepest for N2/N3. This is a result of the strength of the exposedness and hiddenness of particular nodes. N0/N5 are only hidden and N2/N3 are the most exposed and the most hidden nodes.

With RTS/CTS enabled (Fig. 8b), N2/N3 have a slightly different frame dropping probability for Vo and BE. Also a smaller difference for N1/N4 and N0/N5 between Vo and BE can be noticed. The dropping probability for N0/N5 for BE is non zero for the total offered load exceeding 0.75 MB/s, and for Vo – 0.22 MB/s. However, in general, frame dropping probability increases for BE and decreases for Vo (it increases slightly only under light network load for N0/N5 and N1/N4) in comparison with RTS/CTS disabled. The performance of Vo flows can be explained by the small values of EDCA access parameters which lead to more frequent medium access attempts. Obviously, this time DATA transmissions can be successful more often than with RTS/CTS disabled due to the small lengths of the RTS and CTS signaling frames in comparison to DATA frames. The performance of BE can be explained by the increased signaling overhead which causes that DATA frames to wait in the MAC queues for the successful RTS/CTS exchange. The increased overhead for Vo is not as meaningful because of the incomparable gain from successful transmissions of DATA frames. Due to the fact that the frame dropping probability curve's slopes are very similar to the previous ones, the explanation is the same and the strength of the exposedness is the main reason to blame.

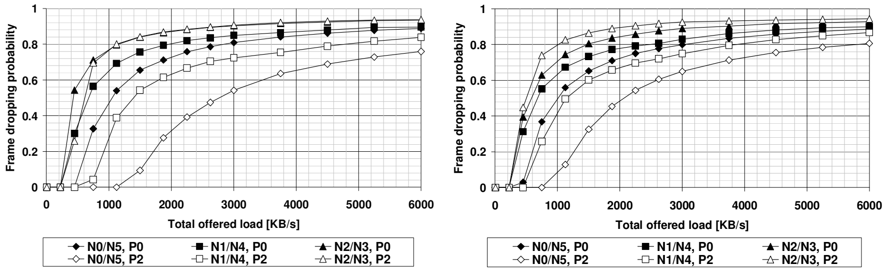

Fig. 8. Six-node line. Frame dropping probability for RTS/CTS (a) disabled (b) enabled.

For the sake of further conclusions, it is important to stress that the strongest hiddenness and exposedness can be observed for N2/N3, weaker for N1/N4, and weakest for N0/N5. However, nodes N0 and N5 hear only N1 and N4, respectively, and nodes N1/N4 hear twice as many nodes each.

The number of retransmission drops (c.f., Fig. 10a-b) is a result of the transgression of the long retry limit (equal to 7, for RTS/CTS enabled) or short retry limit (equal to 4, for RTS/CTS disabled). When the number of retransmissions is compared with the number of collisions (c.f., Fig. 9a-b) for particular nodes it is easily noticeable that with the RTS/CTS exchange disabled the number of retransmissions is in line with the number of collisions for all of the nodes. With RTS/CTS enabled the situation changes drastically. The order of curves representing collisions is completely reverse to those representing retransmissions. This is caused by the fact that in this situation the RTS frames collide instead of the DATA frames. It is also evident that, in comparison to all other nodes, the number of retransmissions decreased most meaningfully for N0/N5 and less meaningfully for N2/N3. Such a behavior leads to a conclusions that with RTC/CTS enabled the hiddenness of nodes is weakly and the exposedness is strongly evident.

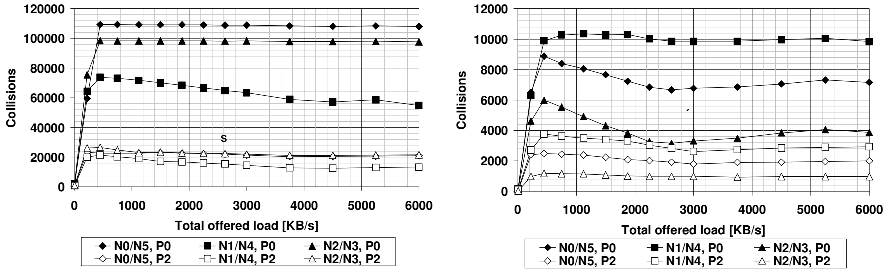

Fig. 9. Six-node line. DATA collision drops for RTS/CTS (a) disabled RTS/CTS (b) enabled.

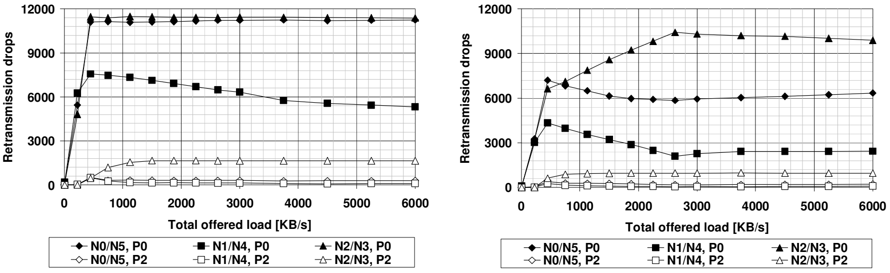

Fig. 10. Six-node line. Retransmission drops for RTS/CTS (a) disabled (b) enabled.

Duplicate drops are a result of collisions of either DATA and ACK frames (in the case of RTS/CTS disabled) or RTS and ACK frames (in the case of RTS/CTS enabled) caused mainly by the exposedness of nodes. The exact reason is that the duration of ACK frames together with SIFS is shorter than AIFS. Consequently, every exposed node can start its transmission of a DATA or RTS frame to a destination node before this destination node receives an ACK from its other neighbor. Collisions on ACK frames cause the node which does not receive the ACK to send its DATA frame once again. As a result, the node which previously sent an ACK frame (which collided) receives the same DATA frame. After the node checks that it already has this frame, it will drop it.

As can be seen in Fig. 11, with RTS/CTS disabled, a meaningful number of duplicate drops can be noticed only for N1/N4. This is because N0/N5 are not exposed at all and N2/N3 are most strongly exposed and hidden. Therefore, the frame transmissions triggered by N2/N3 are in many cases either strongly delayed, collide or are simply impossible. With RTS/CTS enabled, the number of duplicate drops decreases by half for N1/N4 and increases for N2/N3. Similarly as in the case of retransmission drops, this is because introducing RTS/CTS reduces the number of collisions of DATA frames of N2/N3, decreases their hiddenness and emphasizes the exposed nature of N2/N3.

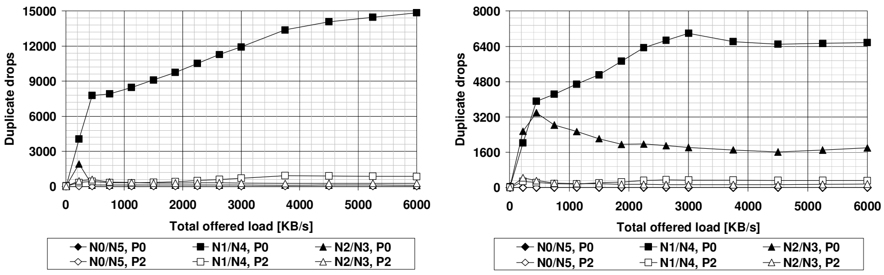

Fig. 11. Six-node line. Duplicate drops for RTS/CTS (a) disabled RTS/CTS (b) enabled.

4.8. Comparison with Star Topology Networks

When the behavior of line topology networks is compared with the behavior of star topology networks (presented in [5]) several important joined conclusions appear. Fist of all, in both cases the strong unfairness in granting medium access between particular nodes is present. Second of all, the order of throughput levels of different priority streams is reverse to the desirable ones (i.e., those expected by IEEE 802.11e). Finally, the employment of the RTS/CTS exchange does not bring meaningful changes because it does not eliminate the aforementioned problems.

The behavior of three- and four-node line topologies is most similar to the behavior of four- and five-node star topology networks. In these configurations nodes being in the middle of the network are favored over the edge nodes. In all other cases the performance of line topologies changes. This is because the importance of the exposed nature of certain nodes (especially the middle ones) grows. Additionally, also the strength of the hiddenness of the middle nodes grows as the line length increases. These two factors cause the medium access of the middle nodes to be strongly hindered. The transmissions triggered by the middle nodes either collide, are strongly delayed or even blocked.

5 General Conclusions

This paper presents a novel simulation study of five different line topology networks based on IEEE 802.11e. The impact of hiddenness and exposedness of particular nodes is commented in details. Moreover, the paper argues the usefulness of the employment of the RTS/CTS mechanism in such networks. In both cases, with RTS/CTS enabled or disabled, nodes sending high priority traffic obtain lower throughput levels than the corresponding ones with low priority streams. Furthermore, high unfairness in medium access between different line-forming nodes is stressed. The general prioritization patterns of nodes are presented in Fig. 12.

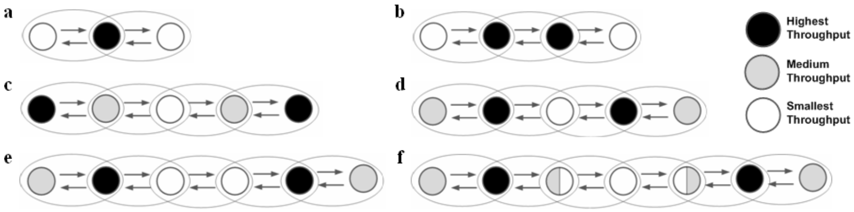

Fig. 12 Prioritization order in (a) three- (b) four- (c) five- (low priority traffic) (d) five- (high priority traffic) (e) six-, and (f) seven-node line.

As can be easily noticed, the higher the number of nodes the more the middle ones are harmed in terms of throughput. Consequently, it can be noticed that it seems impossible for the side nodes to obtain meaningful dominance over other nodes when there are more than four nodes in a line. It can be also expected that similar behavior will occur when the line will be lengthened for RTS/CTS both enabled and disabled.

Additionally, the presented line topology networks are compared with previously analyzed star topology networks. Several joined conclusions are revealed and the main differences are highlighted. The cause of the differences is also explained.

Even though the presented analysis is rather thorough, there is a need for further simulations. The behavior of line topology networks should be checked when the most harmed nodes, in terms of access prioritization, will generate the high priority traffic, while the prioritized ones will generate low priority traffic. Such analysis should be done in order to check if simple changes of EDCA access parameters is a good direction in solving hidden/exposed node problems within IEEE 802.11e based networks. Additionally, other topology networks (more spontaneous than star and line) should be taken into account. Future work will also comprise an analysis of new scenarios to provide even more general conclusions. The overall aim of the planned analysis is to show which threats are most dangerous, and which EDCA factors are most important in building a new mechanism eliminating the degrading impact of hidden/exposed nodes on IEEE 802.11e.

Disclaimer This work has been realized under the Polish Ministry of Science and Higher Education project no. N51739133.

References

1. IEEE 802.11e: *Medium Access Control (MAC) Quality of Service Enhancements*, New York, IEEE Inc., November 2005.
2. IEEE 802.11b: *Higher-speed PHY extension in the 2.4 GHz band*, 1999.
3. TKN EDCA 802.11e extension. http://www.tkn.tu-berlin.de/research/802.11e_ns2, 2006.
4. X. Bai and Y. M. Mao, *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 Computing 2007, WiCom 2007, pp. 1479-1483, September 2007.
5. K. Kosek, M. Natkaniec, L. Vollero, and A. R. Pach, *An Analysis of Star Topology IEEE 802.11e Networks in the Presence of Hidden Nodes*, in Proc. The International Conference on Information Networking 2008, ICOIN'08, Korea, January 2008.
6. V. Bharghavan, A. Demers, S. Shenker, and L. Zhang, *MACAW: A Media Access Protocol for Wireless LAN's*, ACM SIGCOMM'94, UK, September 1994.
7. F. Talucci, M. Gerla, and L. Fratta, *MACA-BI (MACA by invitation) - A Receiver Oriented Access Protocol for Wireless Multihop Networks*, in Proc. IEEE PIMRC'97, Finland, September 1997.
8. Y. Wang and J. J. Garcia-Luna-Aceves, *A New Hybrid Channel Access Scheme for Ad Hoc Networks*, MedHocNet'02, Italy, September 2002.
9. F. A. Tobagi and L. Kleinrock, *Packet switching in radio channels: Part II–The hidden terminal problem in carrier sense multiple-access and the busy-tone solution*, IEEE Transactions on Communications, December 1975.
10. Z. J. Haas and J. Deng, *Dual Busy Tone Multiple Access (DBTMA) – A Multiple Access Control for Ad Hoc Networks*, IEEE Transactions on Communications, June 2002.
11. C. L. Fullmer and J.J. Garcia-Luna-Aceves, *Solutions to Hidden Terminal Problems in Wireless Networks*, in Proc. ACM SIGCOMM'97, France, September 1997.
12. K. Mittal and E. M. Belding, *RTSS/CTSS: mitigation of exposed terminals in static 802.11-based mesh networks*, 2nd IEEE Workshop on Wireless Mesh Networks 2006, WiMesh 2006, USA, 2006.