Performance of an IEEE 802.16 Wireless Backhaul in the Presence of a Node Failure

Pey San Nancy Chai, Kah-Seng Chung and King-Sun Chan
Department of Electrical and Computer Engineering,
Curtin University of Technology
Perth, Western Australia.
p.chai@postgrad.curtin.edu.au, k.chung@curtin.edu.au, and k.chan@exchange.curtin.edu.au

Abstract—**A wireless backhaul network is used to interconnect intermediate nodes to gateway nodes. As it is designed to serve a large population of broadband users, failure sustainability becomes an essential requirement to ensure uninterrupted telecommunication services even in the presence of occasional node or link failures. In this paper, the performance of a failure sustainable wireless backhaul, based on IEEE 802.16 radio technology, is analysed in the presence of a node failure. Furthermore, it is shown that the network performance is significantly improved by incorporating two proposed modifications, namely request-resend and dynamic mini-slot allocation, in IEEE 802.16 standard coordinated distributed scheduling.**

Keywords - wireless backhaul; failure sustainability; scheduling

I. Introduction

Backhaul networks are used to interconnect intermediate nodes to gateway nodes which are located in regional or metropolitan centres [1]. Conventionally, these backhaul networks are established using metallic cables, optical fibres, microwave or satellite links. With the proliferation of wireless technologies, multi-hop wireless backhaul networks emerge as a cost effective and flexible solution to provide extended coverage to areas, such as the difficult to access and sparsely populated rural areas, which have little or no existing wired infrastructure. Deployment of wire line backhaul to such remote areas is often difficult or cost-prohibitive.

Nevertheless, wireless backhaul networks are vulnerable to node or link failures. Additional nodes and links are required to provide alternative paths to ensure undisrupted traffic transmission during failure conditions. Several studies have been carried out to design failure sustainable wireless backhaul [2-5]. A ladder topology, which has a high degree of failure sustainability and can provide at least one backup path between each nodes pair, is proposed in [6]. The performance of such a topology under normal operation, in terms of achievable throughput and average delay, has been presented in [6]. In the same paper, the authors proposed a reverse notification scheme to overcome the severe hidden node problem associated with IEEE 802.16 standard Coordinated Distributed Scheduling (CDS) [7].

In contrast to [6], this paper focuses on the performance analysis of the ladder topology under failure conditions. With the use of computer simulations, it is shown that CDS does not perform well during failure condition. Hence, two new schemes, namely request-resend and dynamic mini-slot allocation, are proposed and incorporated in the standard IEEE 802.16 CDS and the previously proposed reverse notification. Computer simulations have verified that the use of these schemes can greatly enhance the network performance.

The rest of the paper is organised as follows. In Section II, the performance achieved through the use of the standard CDS in conjunction with reverse notification during failure condition, and the problems encountered are described. The proposed request-resend and dynamic mini-slot allocation schemes are presented in Section III. Section IV shows the computer simulated performance achieved with these new schemes, and finally Section V concludes this paper.

II. Performance of IEEE 802.16 and Reverse Notification During Node Failure

A. Simulation settings

An example of the ladder topology proposed in [6] is shown in Fig. 1. This wireless backhaul topology interconnects two distant communities, X and Y, and each intermediate node or link has at least one backup path.

By utilising CDS and the reverse notification scheme, the performance of this topology under a single node failure condition is evaluated using NCTUns network simulator [8]. Constant bit rate (CBR) user datagram protocol (UDP) traffic is used as the data source and this traffic is sent from community X to Y via the intermediate nodes. The data bit rate applied is calculated using the same procedure as described in [6] to achieve a packet loss rate of less than 0.003%. Table I shows the parameters adopted for the simulation.

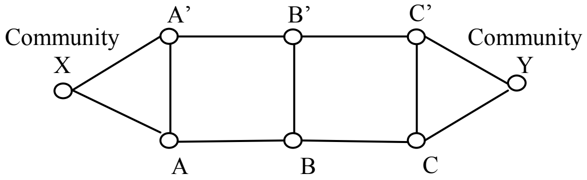

Figure 1. A four-hop ladder topology.

978-1-4244-7005-1/10/$26.00 ©2010 IEEE

TABLE I. SIMULATION PARAMETERS

Parameter	Value
MSH-CTRL-LEN	8
MSH-DSCH-NUM	8
Reservation Frame Length	128
Modulation/Coding Scheme	64QAM-3/4
Frame Duration	10ms
Number of Mini-slot per Frame	220
Total Number of Packets	600000
Packet Size	1000 bytes
Queue Buffer Length	1000 packets
Request Size	40

B. Simulation results

The performance of the four-hop ladder topology, as shown in Fig. 1, during a node failure has been evaluated in terms of the maximum achievable throughput, and the average packet transmission delay. The throughput is determined based on the use of a maximum traffic load that a given ladder topology can support while maintaining no or near zero packet loss. The choice of zero or very low packet loss as the reference is to reflect the main consequence of the hidden node problem, which gives rise to excessive packet queues at network nodes. Such packet queues occur when data packets are being retained from transmissions at the network nodes where the requested mini-slots are not readily available. As the packet queue length increases, data packets have to wait in the queue for long period of time and this increases their transmission delays. Also, when a queue is longer than the buffer size used, packets will be dropped resulting in network throughput degradation.

From the simulation, it is observed that the achievable throughput and delay performance vary with the location of the failure. However, failure at any one of the two nodes in each location shown in Fig. 2 gives similar performance. Table II tabulates the throughput and average delay obtained with the node failure occurred at different node locations.

From Table II, it is observed that a node failure at location 3 has the greatest impact on the network throughput. On the other hand, a better performance is achieved when a node failure occurs at location 2. This is due to the hidden node problem being more likely to happen when a node failure occurs at location 3. Furthermore, the potential hidden nodes encountered by other nodes in the network of Fig. 2 in the event of a node failure have been identified and tabulated in Tables III to V. Note that node Y is not involved with data transmission, and therefore it does not encounter the hidden node problem.

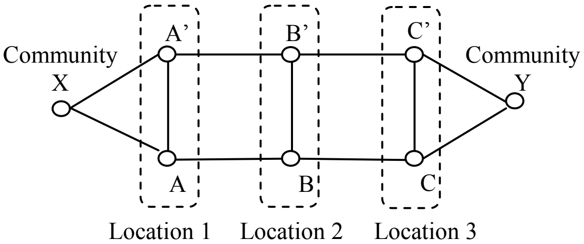

Figure 2. Failure locations in the four-hop ladder topology.

TABLE II. THROUGHPUT AND DELAY ACHIEVED WHEN A NODE FAILURE OCCURRED AT A DIFFERENT LOCATION

Location	Throughput (Mbps)	Average end-to-end delay (ms)
1	8.18	51.66
2	9.11	78.91
3	6.81	41.84

TABLE III. HIDDEN NODES ENCOUNTERED BY A GIVEN NODE WHEN NODE A IN LOCATION 1 FAILS

Node	Potential hidden nodes	Number of hidden nodes
X	B'	1
A'	B, C'	2
B'	X, C	2
B	A', C'	2
C'	A', B	2
C	B'	1

TABLE IV. HIDDEN NODES EXPERIENCED BY A GIVEN NODE WHEN NODE B IN LOCATION 2 FAILS

Node	Potential hidden nodes	Number of nodes
X	B'	1
A'	C'	1
A	B'	1
B'	X, A, C	3
C'	A'	1
C	B'	1

TABLE V. HIDDEN NODES ENCOUNTERED BY A GIVEN NODE WHEN NODE C' IN LOCATION 3 HAS FAILED

Node	Potential hidden nodes	Number of nodes
X	B', B	2
A'	B	1
A	B', C	2
B'	X, A, C	3
B	X, A'	2
C	A, B'	2

Table VI summarises the number of potential hidden nodes together with the corresponding number of occurrences according to the location when a node failure occurs.

TABLE VI. NUMBER OF POTENTIAL HIDDEN NODES AND THEIR NUMBER OF OCCURRENCES

Number of hidden nodes	Number of occurrences		
	Location 1	Location 2	Location 3
1	2	5	1
2 or above	4	1	5

From Table VI, it is observed that in the event of a node failure occurring at location 2, the other nodes in the backhaul are likely to be associated with a single hidden node. On the other hand, when a node at location 3 fails, there is the greatest chance that the other nodes will have two or more hidden nodes associated with them. As such, it elevates the hidden node problem and makes the reverse notification scheme less effective. Under this condition, it is necessary to reduce the amount of traffic applied to the backhaul in order to maintain the near zero packet loss. Now, with a lower traffic load, the throughput is reduced but the traffic will experience less delay as fewer data packets are in the queue at each node. This explains the observation that when a node failure occurs at location 3 the resultant throughput and delay are lower.

In order to increase the achievable throughput, it is necessary to enhance the reverse notification scheme in an attempt to minimise the frequency of occurrences of the hidden node problem. As such, a request-resend procedure is proposed to be incorporated into the reverse notification scheme and it will be explained in details in Section III.

Furthermore, it has been observed that in the event of a node failure, the neighbours of the failed node will have to handle a large amount of rerouted data traffic. As a result, these nodes will become the bottlenecks for traffic congestion if their bandwidth allocation remains the same as other non-neighbouring nodes of the failed node. However, this issue can be overcome by adopting a dynamic mini-slot allocation scheme which allocates the number of data mini-slots to a given node according to its servicing traffic. This dynamic mini-slot allocation scheme is described in Section III.

III. Request-resend and Dynamic Mini-slot Allocation

A. Request-resend

The IEEE 802.16 standard specifies that the coordinated distributed scheduling employs a three-way (TW) handshaking procedure for setting up connections between neighbouring nodes [7]. During this handshaking, a sending node, say node R in Fig. 3, first informs the intended receiving node, i.e., Node S in this case, the frames and mini-slots, which are available for it to transmit data. Upon receiving the request, node S will then determine whether these requested frames and mini-slots are free for data reception. At the same time, node Q also overhears the handshake between node R and node S. During the mean time, it is possible that another sending node, say node P, might request for the same resources as Node R to forward its data packets to node Q. With node P being two hops away from node R, it therefore would not be aware of the request of node R. Consequently, the request of node P will not be granted by node Q. This scenario is commonly referred as the hidden node problem.

A reverse notification scheme, as shown in Fig. 4, has been proposed in [6] to overcome this hidden node problem. With this reverse notification, each individual node is informed of the mini-slots occupied by all its two-hop neighbours. Hence, this can prevent two nodes, which are two hops away, from requesting the same mini-slots. However, there is a possibility that the reverse notification might fail to reach the relevant node in time to prevent it from making the conflicting request. This scenario is illustrated in Fig. 5.

In an attempt to overcome the scenario of Fig. 5, a request-resend scheme is proposed to operate in conjunction with reverse notification. With this scheme, as illustrated in Fig. 6, after receiving a reverse notification from node Q, node P will send a new request specifying a different set of mini-slots from node R. This allows node Q to grant node P its requested mini-slots. Consequently, node P is able to transmit its traffic straight after confirming the grant to node Q.

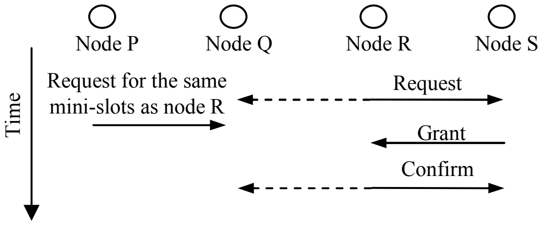

Figure 3. Hidden node problem.

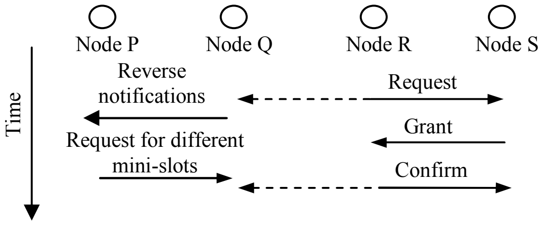

Figure 4. Reverse notification scheme.

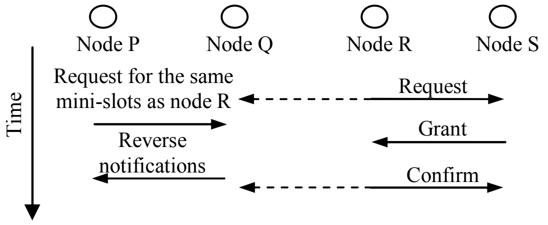

Figure 5. A scenario where the reverse notification scheme fails to prevent two two-hop neighbouring nodes from making the same resource request.

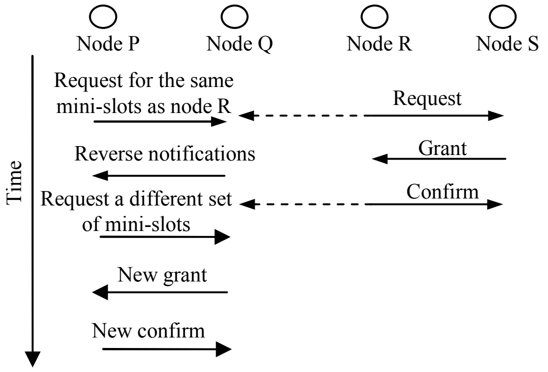

Figure 6. Request-resend scheme.

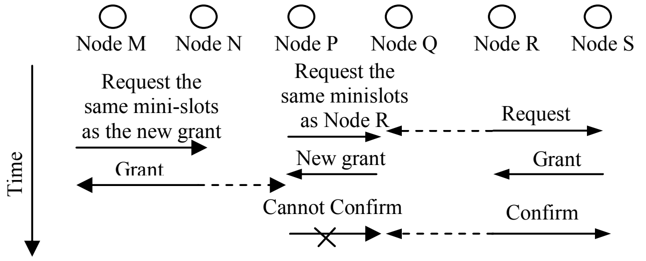

Figure 7. Possible hidden node problem when request-resend is not used.

Now, consider the situation where there are two additional nodes, M and N, before node P, as shown in Fig. 7. If node Q sends a new grant straight after receiving the first request from node P without any knowledge of the request from node M to node N, a second hidden node event might occur. In this case, the new grant will cause conflict at node N as collision will occur at node N if nodes P and M transmit at the same time. Thus node P cannot confirm the new grant. With the use of request-resend, instead of node Q deciding on the mini-slots for node P to transmit data, node P will determine the set of available mini-slots that are not in conflict with node M for its own packet transmission. Node P is able to derive the information on non-conflicting mini-slots from the grant message of node N to node M and the reverse notification from node Q. Hence, the use of request-resend in conjunction with reverse notification will effectively overcome the hidden node problems.

B. Dynamic mini-slot allocation

When a failure occurs, traffic will be rerouted bypassing the faulty node to reach the final destination via alternative paths. Hence, neighbours of the failed node are likely to handle a larger amount of traffic. These nodes will become bottlenecks unless they are allowed to request for more mini-slots. Conversely, those nodes that are not involved in rerouting traffic may need to decrease their share of mini-slots. As such, a dynamic mini-slot allocation scheme is proposed for adjusting the mini-slot allocations according to the traffic loads serviced by individual nodes in the event of a node failure. The operation of this dynamic mini-slot allocation scheme is described as follows.

- Under normal operation, a node will hold off for a period of time after sending a control message. If a node does not send a control message within two hold off periods, it is regarded as a failed node.
- Upon detecting a failed node, the node preceding it will divert the traffic via an alternative path to another node. At the mean time, it will decrease its request mini-slot size. This node will also reduce the number of mini-slots granted for its upstream nodes as well as issuing a node failure notification flag in the grant information element (IE). This flag is realised using a single bit in the grant IE.
- When a grant IE with a failure flag is received by the node that the message is destined for, it will reduce the amount of mini-slots granted to its upstream neighbors to be the same as it has received from its downstream node. Once again, the failure flag will also be included in the grant IE for passing on to the next upstream node. In this way, the failure flag will be propagated to all the operating nodes within the network. This will then allow each node to readjust the amount of mini-slots it could grant.
- When a node receives a request from an upstream node which under normal operating conditions is not supposed to relay traffic to it, it knows that it has to handle an additional rerouted traffic. As such, it will increase its request for mini-slots to its downstream node by doubling its normal request size in order to accommodate the additional traffic.
- As specified in the IEEE 802.16 standard, only mini-slots in a continuous range can be handled by the requesting and granting nodes during a three way handshake. This makes it difficult to realize dynamic mini-slot allocation. For this reason, the three-way handshake procedure is modified to enable the requesting and granting nodes to handle multiple discontinuous sets of mini-slots to meet their resource requirements. In an attempt to prevent a node from monopolizing the network bandwidth, a limit is placed on the maximum number of times the node is allowed to request or grant mini-slots in a three-way handshake. Based on the observation made from computer simulation, an appropriate limit is two times.

IV. Performance Evaluation of Request-resend and Dynamic Mini-slot Allocation

In this section, the performance of the standard IEEE 802.16 CDS incorporated with reverse notification, request-resend, and dynamic mini-slot allocation is first evaluated using the four-hop ladder topology of Fig. 2 under a single node failure condition. This has been carried out using the NCTUns network simulator [8] based on the simulation settings described in Section II. Furthermore, the theoretical throughput is also calculated by estimating the amount of mini-slots allocated to each link during a node failure. This is achieved by determining the collision domain set (CoDS) for each link in the network. The CoDS of a given link is defined as the number of links, including itself that are potentially in conflict for channel resource. For example, in a four-hop ladder topology, by assuming node C has failed, the maximum CoDS is observed at L_3 and L_5 as illustrated in Fig. 8. Since link L_3 and L_5 have the largest CoDS, these links are likely to be the bottlenecks, which influence the maximum throughput of the network. By dividing the total mini-slots with the maximum CoDS, the number of mini-slots can be allocated to link L_3 and L_5 is 31. The maximum throughput is given by:

$$\text{Throughput} = \frac{2 \times r_s \times m_b}{T_f} \quad (1)$$

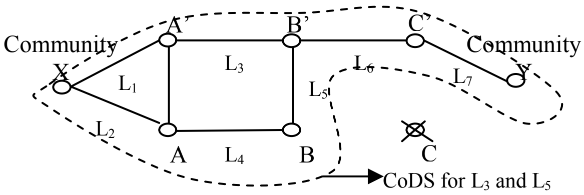

Figure 8. CoDS for L_3 and L_5.

TABLE VII. THROUGHPUT AND AVERAGE DELAY OBTAINED AFTER INCORPORATING REVERSE NOTIFICATION, REQUEST-RESEND AND DYNAMIC MINI-SLOT ALLOCATION INTO THE STANDARD IEEE 802.16 COORDINATED DISTRIBUTED SCHEDULING

Failure location	Throughput (Mbps)			Average end-to-end delay (ms)
	CDS and reverse notification	Request-resend and dynamic mini-slot	Theoretical throughput	
1	8.18	13.6	15.33	138.66
2	9.11	13.6	15.33	138.96
3	6.81	13.6	15.33	138.91

TABLE VIII. PERFORMANCE COMPARISON UNDER NORMAL AND SINGLE NODE FAILURE CONDITIONS

Number of hops	Normal		A single node failure	
	Throughput (Mbps)	Delay (ms)	Throughput (Mbps)	Delay (ms)
2	25.80	68.79	25.80	70.66
3	25.80	98.75	16.33	110.76
4	20.00	110.61	13.60	138.84
5	20.00	129.15	13.20	148.07
6	16.02	140.18	12.91	152.62

where r_s is the number of allocated mini-slots, m_b is the number of bits that can be transmitted in a minislot, and T_f is the frame duration. The throughputs and average delays obtained using simulation and theoretical calculation with the node failure occurring at different node locations in the four-hop backhaul are tabulated in Table VII. From Table VII, it is observed that the adoption of the proposed request-resend and dynamic mini-slot allocation has greatly enhanced the throughput. More importantly, the throughput remains constant regardless of the location of the node failure and the value is closer to the theoretical maximum. These observations verify that the hidden node problem has largely been mitigated by the request-resend scheme, and the channel bandwidth utilisation is also improved with the use of dynamic mini-slot allocation. Now, with the backhaul being able to support a larger amount of traffic while maintaining no or near zero packet loss, more packets are expected in the buffer queue at each node. As such, this increases the average end-to-end delay.

Next, the effectiveness of the proposed request-resend and dynamic mini-slot allocation schemes has been evaluated for the ladder backhaul with different hop counts. Table VIII shows the throughputs and the average end-to-end delays achieved when the backhaul is operating either normally or with a single node failure. As observed in Table VIII, there is a reduction in throughput when the number of hops of the backhaul is increased. This occurs when the backhaul is operating normally or in the presence of a single node failure. This is due to the fact that when the hop count is increased, the amount of mini-slots allocated to each node is correspondingly decreased. As expected, all the topologies, with the exception of the one with two hops, suffer a decrease in throughput during a node failure. For the two-hop topology, the total number of mini-slots allocated to each hop remains the same even when there is a node failure. But for all the other topologies, those nodes that are not involved in traffic rerouting will have their share of mini-slots reduced. Consequently, the achievable throughput is reduced. At the same time, the average delay is increased as the amount of data can be sent in a period of time is reduced.

V. CONCLUSION

The performance of the IEEE 802.16 standard Coordinated Distributed Scheduling (CDS) incorporating a previously proposed reverse notification scheme is evaluated for a failure sustainable wireless backhaul with a ladder topology. Computer simulations show that there is a significant reduction in throughput when the network encounters a node failure. Furthermore, the achievable throughput is affected by the actual location of the single node failure.

In this paper, two proposed modifications, namely request-resend and dynamic mini-slot allocation, are added to the CDS and reverse notification. As a result, the achievable throughput of the wireless backhaul is greatly increased, and its value remains constant irrespective of where the single node failure occurs.

REFERENCES

[1] Y. Zhuang, K. Tan, V. Shen, and Y. Liu, "VoIP aggregation in wireless backhaul networks," in IEEE International Conference on Communications, Istanbul, Turkey, pp. 5468-5473, June 2006.

[2] Y. Bejerano and D. Qunfeng, "Distributed construction of fault resilient high capacity wireless networks with bounded node degree," in IEEE International Conference on Computer Communications, Rio de Janeiro, Brazil, pp. 2646-2650, April 2009.

[3] G. Egeland and P. E. Engelstad, "The economy of redundancy in wireless multi-hop networks," in IEEE Wireless Communications and Networking Conference, Budapest, Hungary, pp. 1-6, April 2009.

[4] P. Leesutthipornchai, N. Wattanapongsakorn, and C. Charnsripinyo, "Efficient design techniques for reliable wireless backhaul networks," in International Symposium on Communications and Information Technologies, Vientiane, Lao, pp. 22-27, October 2008.

[5] W. S. Soh, Z. Antoniou, and H. S. Kim, "Improving restorability in radio access network," in IEEE Global Telecommunications Conference, San Francisco, USA, pp. 3493-3497, December 2003.

[6] P. S. N. Chai, K. S. Chung, and K. S. Chan, "Failure sustainable wireless backhaul," in 15th Asia-Pacific Conference on Communications, Shanghai, China, pp. 871-875, October 2009.

[7] "IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems," IEEE Std 802.16-2004 (Revision of IEEE Std 802.16-2001), pp. 0_1-857, 2004.

[8] S. Y. Wang, et al., "The design and the implementation of the NCTUns 1.0 network simulator," Computer Networks, vol. 42, pp. 175-197, June 2003.