Failure Sustainable Wireless Backhaul

Pey San Nancy Chai, Kah-Seng Chung and King-Sun Chan

Department of Electrical and Computer Engineering, Curtin University of Technology, Perth, WA
p.chai@postgrad.curtin.edu.au, k.chung@curtin.edu.au, and k.chan@exchange.curtin.edu.au

***Abstract*-Backhaul network plays a significant role to interconnect access points and further connect them to gateway nodes. A failure sustainable wireless backhaul topology is proposed to ensure undisrupted telecommunication services even in the presence of occasional node or link failures. Furthermore, a new control message, called reverse notification, is proposed to improve the performance of coordinated distributed scheduling in the ladder topology. Computer simulation results show that the reverse notification scheme has improved the network throughput and reduced the packet transmission delay.**

Keywords—**Wireless backhaul, failure sustainability, scheduling.**

I. INTRODUCTION

Backhaul networks are used to interconnect access points and further connect them 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 where the deployment of wireline backhaul is difficult or cost-prohibitive such as the difficult to access and sparsely populated remote areas, which have little or no existing wired infrastructure.

Nevertheless, wireless backhaul networks are vulnerable to node or link failures. In order to guarantee undisrupted traffic transmission even in the presence of failures, additional nodes and links are used to create alternative paths between each source and destination pair. Moreover, the deployment of such extra links and nodes requires careful planning to ensure that available network resources can be fully utilised while still achieving the specified failure sustainability with minimum infrastructure establishment cost. Thus the first contribution of this paper is the design of a failure sustainable backhaul topology, which is aiming to transport traffic between two distant communities typically found in remote areas. This topology is explained in details in Section II.

In order to evaluate the performance of the proposed network topology, IEEE 802.16 [2] standard is chosen as it can provide high network capacity over long distances. In this standard, time division multiple access (TDMA) technology is used where each frame is divided into control and data subframe. Two type of scheduling are used in this standard, namely centralised and distributed scheduling. Distributed scheduling is further divided into two operation modes, namely the coordinated and uncoordinated modes. This paper focuses on analysing the performance of coordinated distributed scheduling in the proposed topology.

It has been pointed out in [3] that all wireless networks, including IEEE 802.16 networks, suffers from hidden terminal problem. This problem retains nodes from data transmission for a long period of time causing data packet queues to build up at these nodes. As a result, packets transmission delay increases and packets maybe dropped due to buffer overflows. As a result, the network throughput is significantly reduced.

In [4] and [5], attempts have been made to improve the minislots allocation efficiency in coordinated distributed scheduling. A throughput-efficiency optimal distributed data subframe scheduling has been proposed in [4] to maximise the throughput of all connections while achieving fairness between connections. Unlike the continuous minislot allocation scheme specified in the standard [2], a multi-grant (MG) scheme has been proposed in [5] to allow multiple discontinuous minislots allocation. With this scheme, it is necessary for individual nodes to specify a large minislot range in their availability information elements (IEs).

This paper introduces a new control message, called reverse notification, to overcome the hidden terminal problem in the minislots allocation procedure as well as avoiding the need for a requesting node to ask for an overly large available minislot set in its availability IE. The proposed scheme makes it possible for a requesting node only to specify the number of available minislots equal to the request size. Hence, this increases the reuse of the minislots in the network. With this new control message, neighbouring nodes are able to avoid sending the same request and availability IEs thus increasing the chance for requesting nodes to obtain all their requested resources. Also, it enables transmitting nodes to initiate data transmission as soon as the handshake is complete. Computer simulations have verified that the use of this reverse notification can significantly reduce the hidden terminal problem and thus maximises concurrent

978-1-4244-4785-5/09/$25.00 ©2009 IEEE

transmissions to increase network throughput and reduce transmission delays.

The rest of the paper is organized as follows. Section II describes the proposed failure sustainable wireless backhaul topology. Section III explains coordinated distributed scheduling and the hidden terminal problem. Section IV explains the proposed reverse notification control message. Simulation results are presented in Section V and finally Section VI concludes the paper.

II. Failure Sustainable Wireless Backhaul

In order to establish a failure sustainable wireless backhaul, there are several criteria that should be considered namely deployment cost, the degree of sustainability, additional transmission delay occurs during failures and the interference generated by additional links and nodes. The deployment cost should be minimised by keeping the number of nodes and links to minimum while providing certain degree of failure sustainability. Degree of sustainability is measured by the number of backup paths between each source and destination pair. Different applications require different degree of failure sustainability. As wireless backhaul networks serve a large population of broadband users, it is essential to provide at least a backup path for each nodes pair. Furthermore, the additional transmission delay incurs when traffics are rerouted should be minimised by reducing the number of extra hops the traffic needs to transverse during failures. Also, it is crucial to keep the number of additional links and nodes to a minimum in order to reduce interference. This paper investigates the use of a relatively simple ladder topology, which meets the above requirements, for establishing a failure sustainable wireless backhaul connecting two distant communities. A six-hop ladder topology is shown in Fig. 1. It consists of two chains of relay nodes, namely A,B,C,D,E, and A',B',C',D',E' serving the two distant gateway nodes, X and Y. On its own, a single chain of relay nodes is sufficient to form the wireless backhaul. However, its operation will be disrupted in the presence of a single node or link failure. This well-known shortcoming of a chain topology can be largely overcome, in this case, by introducing an additional chain of relay nodes to provide at least a backup path for each nodes pair. Such an arrangement only requires the minimum number of additional nodes to realize the necessary back up paths. Furthermore, this ladder topology can sustain multiple link and node failures with the exception of two failure scenarios as illustrated in Fig. 2.

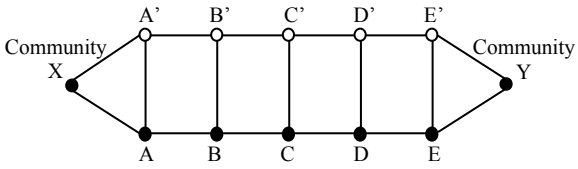

Fig. 1 A six-hop ladder topology.

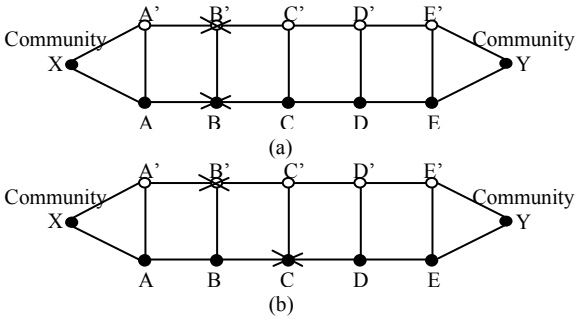

Fig. 2 The two failure scenarios that are not supported by the ladder topology: (a) node or link failures occurring at the same hop level in the two branches, (b) node failures at consecutive hop level in the two branches.

With this ladder topology, traffic packets encounter minimum additional transmission delay in rerouting during node or link failures. For example, if the number of failures in the network is *n*, then the traffic only needs to transverse *n* additional hops. Moreover, for a given node, there are only a maximum of three neighbouring nodes. As such, the channel contention at a given node is likely to increase when compared with a simple chained network.

III. IEEE 802.16 Coordinated Distributed Scheduling

With IEEE 802.16, the coordinated distributed scheduling employs a three-way (TW) handshaking procedure for setting up connections between neighbouring nodes. This procedure is illustrated in Fig. 3.

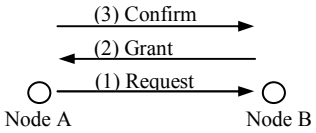

Fig. 3 Three-way handshake procedure in IEEE 802.11.

A TW handshake procedure begins when a node is ready to transmit its data packets. It first sends out a request information element (IE) and the corresponding availability IE to the intended receiving node. The request IE specifies the request size, in terms of the number of minislots required. The availability IE contains a list of consecutive minislots that it believes are available for transmission. Upon receiving these two IEs, the receiving node will determine whether the minislots are actually available for data reception. In the event of unable to allocate the minislots required by the requesting nodes, the receiving node will either ignore the request or allocate fewer minislots than what have been requested. Then, the receiving node will send to the requesting node a grant IE specifying the allocated minislots. The completion of the TW handshake takes place once the requesting node accepts the minislots allocation by sending a confirm IE, which is a duplicate copy of the grant IE, back to the receiving node. The

exchanges of IEs during a three-way handshake serve to also notify neighbouring nodes, which are two hops away, that the minislots specified in the IEs are no longer available. In response, they should not request or grant the same minislots for their own data transmission or reception to avoid possible packet collisions. However, this does not totally eliminate the possibility of the same minislots being adopted among the neighbouring nodes. One such scenario is depicted in Fig. 4.

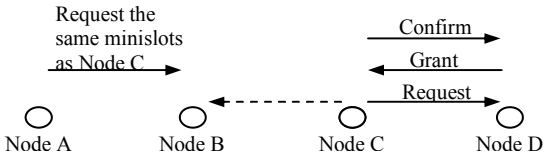

Fig. 4 A scenario of Node C appeared to be hidden from Node A.

In this case, Node A is not aware that Node C has requested the same set of minislots. On the other hand, Node B overhears the IEs exchange between Node C and Node D. This leads to Node B to either reject the request of Node A or grant it the requested minislots after Node C has finished its transmission to avoid packet collisions at node B. As result, Node A is likely to have to wait for its turn to transmit.

A shown in Fig 4, this hidden node problem involve neighbouring nodes that are within three hops. This problem is likely to occur more frequently when the number of nodes within three hops increases. This suggests that a solution is needed to overcome such problem to avoid a drastic degradation in network throughput.

IV. Reverse Notification Control Message

It is proposed that the TW handshake be extended to include a new reverse notification control message to largely overcome the hidden node problem. This control message takes the form of a duplicate copy of availability IE.

A reverse notification control message is sent only after a node has received request and availability IEs that are not destined for it. This control message can be sent in conjunction with either one of the three IEs, i.e., request, grant or confirm, within the control subframe. This is made possible by the fact that a node can send multiple IEs at a given time. In this way, it will increase the likelihood for the destine node to receive the reverse notification message before it attempts to make request for channel resource. An example of the exchange of reverse notification message is shown in Fig. 5. It shows that Node B, which overhears the transmission of request IE by node C, will transmit a reverse notification to node A. Upon receiving this message, Node A will request only those minislots which are not listed in the reverse notification IE. This will then ensure that Node A will be able to obtain its requested resource from Node B. To ensure the hidden terminal problem can be tackled effectively, all the neighbouring nodes of Node C have to send a reverse notification. As the information carried by the reverse notification, which is piggybacked to other IEs, is small and thus the extra overhead and delay incurred are eligible.

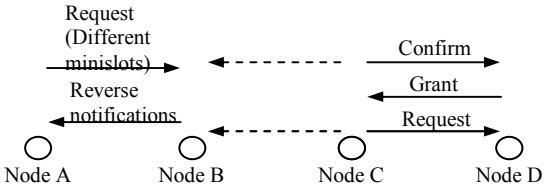

Fig. 5 An exchange of reverse notification control message.

Nevertheless, the inclusion of the reverse notification control message in the TW handshake still does not completely resolve the hidden node problem. For example, if Node A fails to receive the reverse notification message in time before it makes a request for channel resource, then it is possible that it will request for the same minislots that have already been used by its neighbouring nodes. However, it is observed from computer simulations that the occurrence of such an event is pretty infrequent. As such, the proposed extension to the TW handshake is able to significant enhanced the network throughput.

Due to the broadcast nature of a wireless environment, other nodes nearby to the one that broadcast the reverse notification message, say Node B in this case, might also receive the same control message. In such situation, those nodes that intend to send data to Node B will either have to defer making requests for minislots, which have already been occupied, or request for some other available minislots. This is to avoid possible collisions at Node B. On the other hand, those nodes that do not intend to send request to node B will simply drop the reverse notification control message.

V. Performance Evaluation

In this section, the performance of the proposed reverse notification scheme operating in a ladder network is evaluated using the NCTUns network simulator [6]. It is assumed that the network has no node or link failure. Seven ladder topologies with the number of hops ranging from two to eight are evaluated. These results are then compared with those obtained using the original IEEE 802.16 three way handshake protocol.

A. Simulation setup

Table II shows the parameters adopted for the computer simulation. The NCTUns simulator employs a simple procedure for determining the minislot start parameter to be specified by a given node in its availability IE. It begins the search for the first available minislot starting from the first timeslot in a frame. The process continues until a set of available minislots required to fulfil the request size specified by the request

IE is met. Such a search procedure may increase the reuse of minislots within the network and make possible larger number of concurrent transmissions.

TABLE II

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

Different minislot request sizes are needed to cater for different network topologies so that as many of the 220 minislots in a frame will be used by the network. Constant bit rate (CBR) User Datagram Protocol (UDP) traffic is used as the data source from the gateway node X input to the network. A different bit rate is adopted in order to match the amount of traffic load that could be supported by a given network topology. The request size and bit rate for a given ladder topology are calculated as follows.

1) Request size

To ensure fairness, all individual links of a given network are to make use of a fixed request size. In order to calculate the request size, it is necessary to determine the collision domain set (CDS) for each link in the network. The CDS of a given link is defined as the number of links, including itself, that are potentially in conflict for channel resource. As such, all these links will have to allocate or make use of different sets of minislots to avoid collision. The request size for a given network topology can then be calculated as follow:

$$\text{Request size} = \left\lfloor \frac{\text{Total no. of data minislots in a frame}}{\text{Number of links in the largest CDS}} \right\rfloor$$

Now, consider a two-hop ladder topology of Fig. 6, the number of conflicting links, which are links that are within two hops of a given link, is four. This results in CDS being equal to five. Moreover, when there is no node or link failure, the backup link, i.e., link 5 in Fig. 6, is not active, As such, the CDS value for this two-hop ladder network may be reduced from five to four for the calculation of the required request size.

The request size as calculated above is the maximum value and it may not always be applicable to all the network topologies due to the dynamic scheduling of minislots among the network nodes. In such a situation, a smaller value of request size may be used to overcome the influence of the request size on the achievable maximum throughput.

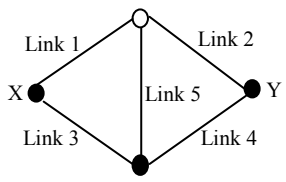

Fig. 6 A two-hop ladder topology having the same CDS for each link.

2) CBR of the UDP traffic

The bit rate of the UDP traffic to be adopted for a given ladder topology can be calculated according to

$$CBR = \frac{\text{No. of bits transmitted in a frame}, B}{\text{Frame duration}, T_f}.$$

The number of bits that can be transmitted in a frame is a function of the viable request size used, and is given by

$$B = r_s \times m_b - o_h$$

Where r_s is the request size, m_b is the number of bits that can be transmitted in a minislot, and o_h is the overhead.

The calculated CBR is an estimation of the maximum traffic load that can be supported by a network before packets starts to be dropped due to buffer overflow. Since the severity of the hidden node problem varies somewhat with network topology, it is necessary to adopt an appropriate CBR for a given network to ensure no or near zero packet loss due to traffic overload. The actual CBR used for a given network topology is obtained by gradually reducing its value until it causes a very small packet loss of less than 0.003%.

B. Simulation Results

The effectiveness of the proposed reverse notification scheme operating in different ladder topologies 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 reference is to reflect the main consequence of the hidden node problem which gives rise to excessive packet queues at network nodes when data packets are being retained from transmission due to the unavailability of their requested minislots. 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.

The maximum achievable network throughputs obtained through the use of the proposed reverse notification scheme in the seven ladder topologies, ranging from two to eight hops, are shown in Fig. 7. For comparison, the throughput values achieved with the original three way handshake protocol are also presented.

From Fig. 7, it can be observed that the hidden node problem can have a great influence on the network throughput. For example, the conventional TW

handshake is able to perform well in a two-hop ladder topology which does not suffer from such problem. However, the network throughput is severely degraded due to the hidden node problems present in networks with more than two hops. On the other hand, the reverse notification scheme is able to improve the network throughput significantly. With this scheme, it is able for the three-hop ladder topology to achieve the same throughput of the two-hop ladder network. However, as the number of hops increases from 4 to 8, the maximum throughputs become smaller. This could be due to the increase in control subframe contentions as the number of nodes increases. This will decrease the likelihood of the reverse notification IEs being received by the relevant nodes before they make channel resource requests.

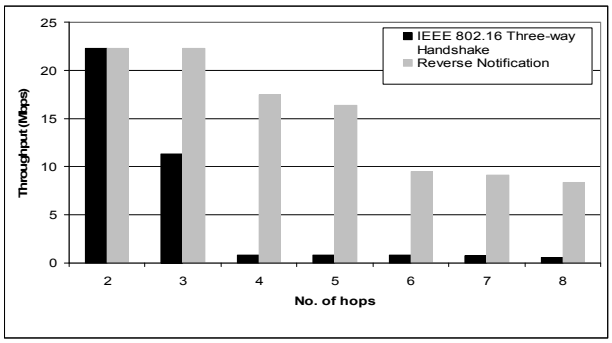

Figure 7. Maximum achievable throughputs obtained with different ladder topologies.

Table III shows the packet transmission delay for different ladder topologies.

TABLE III

PACKET TRANSMISSION DELAY

Delay (ms)			
Number of hops	Request Size	Without Reverse Notification	Reverse Notification
2	50	63.88	59.19
3		24.16	94.15
4	40	317.73	104.78
5		365.75	83.45
6	35	395.64	54.78
7		523.41	61.19
8		545.91	75.70

From Table III, it can be observed that different request sizes are used for different number of hops. Packet transmission delay is compared among topologies with the same request size as similar traffic loads are applied to these networks. For the same request size, it can be observed that the delay increases as the number of hops increases. This is due to traffic needs to traverse a longer path to reach the destination. However, it can be noticed that packet transmission delay for three-hop ladder topology using the original three-way handshake has a smaller packet transmission delay as compared to two-hop ladder topology. This is because packet loss in two-hop ladder topology is caused by packet queue overflow due to excessive load applied to the network. On the other hand, packet loss occurs in three-hop ladder topology due to hidden terminal problem. The same reason applies to the four and five-hop ladder topologies using the reverse notification scheme. The difference between three-hop ladder topology using the original three-way handshake and the reverse notification scheme is caused by higher traffic load is applied when the topology is using reverse notification scheme. Overall, the reverse notification is able to improve the packet transmission delay as compared to the original three-way handshake.

VI. CONCLUSION

A ladder topology has been proposed for a failure sustainable wireless backhaul network which can deliver undisrupted telecommunication services between two distant remote communities. For such a backhaul network, it is shown that the coordinated distributed scheduling procedure as specified in the IEEE 802.16 standard does not perform well in a multihop ladder topology due to the hidden node problem. Such a problem has to a large extend been overcome through the use of the proposed reverse notification scheme. Computer simulations have verified that this reverse notification scheme is able to significantly increase the network throughput and reduce the packet transmission delay. The scheme is also applicable to other network topologies, such as the grid topology. Future work will be carried out to further improve the proposed scheme by making sure that the reverse notification message is able to arrive at potential conflicting nodes before they have to make channel requests. Furthermore, effective ways of rerouting traffic to minimise queue built up at certain nodes will also be investigated.

REFERENCES

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

[2] "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.

[3] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Computer Networks,* vol. 47, pp. 445-487, 2005.

[4] T. Da, Y. Shoubao, H. Weiqing, and H. Yun, "TEOS: A Throughput-Efficiency Optimal Distributed Data Subframe Scheduling Scheme in WiMAX Mesh Networks," in *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on*, 2008, pp. 1-4.

[5] W. Shie-Yuan, L. Chih-Che, and F. Ku-Han, "Improving the Data Scheduling Efficiency of the IEEE 802.16(d) Mesh Network," in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, 2008, pp. 1-5.

[6] S. Y. Wang, C. L. Chou, C. H. Huang, C. C. Hwang, Z. M. Yang, C. C. Chiou, and C. C. Lin, "The design and implementation of the NCTUns 1.0 network simulator," *Comput. Netw.,* vol. 42, pp. 175-197, 2003.