A Switching Architecture for Remote Radio Head Protection in Cloud Radio Access Networks

Qianmei Yang, Calvin Chun-Kit Chan
Department of Information Engineering, The Chinese University of Hong Kong, Hong Kong.
yq013@ie.cuhk.edu.hk

Abstract—Cloud radio access network (C-RAN) is a persuasive solution to the burst capacity in future 5G mobile system and it can tackle the tidal effect in mobile networks for better resource utilization. We propose a remote radio head (RRH) protection scheme to assure the availability of the RRHs. A protection layer is proposed to support re-configurable protection of the RRHs, with good scalability.

Keywords—C-RAN; the tidal effect; RRH protection; optical switch network

I. INTRODUCTION

The next generation 5G mobile network system has a significant feature of high capacity at the mobile user ends. To fulfill this requirement, cloud radio access network (C-RAN) is widely recognized as a potential feasible solution. It separates the baseband units (BBUs) from the remote radio heads (RRHs) and centralizes the BBUs to a BBU pool. Hence, it exhibits several advantages over the traditional approach, such as the ability of functioning coordinated multipoint [1, 2], reducing handovers between adjacent RRHs [3] and decreasing the total power consumption [4, 5]. In the white paper of China Mobile [6], it suggested that C-RAN could also be a potential solution of the tidal effect in mobile networks, caused by the daily commuting of the users between the office area and the residential area. Based on this characteristic of mobile network usage, we have proposed an architecture of BBU pool aiming at reducing the amount of the required BBUs and realizing BBU protection in the system [7]. In order to further realizing the protection of the RRHs, in this paper, we investigate the architecture of the RRH network and propose a feasible solution for protecting the RRHs.

II. PROTECTION OF RRHs

Similar to the mobile network architecture discussed in [7], we assume that the office area and the residential area are sharing the same central office (CO) and the same BBU pool, as illustrated in Fig. 1. At the CO, intensity modulation/direct detection (IM/DD) is employed to support downstream transmission and the RRHs are colorless. As the office area and the residential area have different peak hours of capacity usage, we divide BBUs into static ones and dynamic ones and their serving RRHs are called static RRHs and dynamic RRHs, respectively. The static BBUs constantly serve a particular area while the dynamic BBUs are switched between the two areas to serve the busier area. The static RRHs operate all day long while the dynamic RRHs are shut down during the off-peak time. Hence, the availability of the static RRH network becomes important and thus protection measures for the static RRH network is indispensable.

In the network design, we have the following assumptions, including, (1) the RRHs including both the static and the dynamic are identical; (2) the largest coverage range of a RRH is a circle; (3) the signals from all static RRHs can cover the whole serving area; (4) the dynamic RRHs are supplementary to the static RRHs and they can be used to protect any failed static RRH such that the whole area can still be served completely during peak times; and (5) there is at most one RRH failure at any time. In practical cases, the architecture of the static RRHs depends on the actual situation of the area, we model the distribution of the static RRHs in form of a Voronoi diagram, as shown in Fig. 2(a). According to our assumptions, the distance between a static RRH and the farthest vertex of its own cell should not exceed the coverage radius of the static RRH. To make better use of the dynamic RRHs, we place them at the vertices of the Voronoi diagram.

As it has been assumed that all static and dynamic RRHs should be able to cover the whole area even though any one of the static RRHs fails during peak time, our goal is to use the dynamic RRHs to protect the static RRHs at the off-peak time. First, it would be crucial to investigate the number of dynamic RRHs required to protect one static RRH. We have considered the cases that one static RRH is surrounded by a Voronoi polygon of different number of vertices, each of which may host a dynamic RRH. It has been assumed that such Voronoi
Consider a more strict case in which all the vertices of the polygon are located on the boundary of the circular coverage range of the static RRH. From geometry, if two adjacent vertices have an included angle at the center of no larger than 120°, the two dynamic RRHs located at these two vertices should be able to cover the whole sector area with the included angle of at least 120° and at most 240°, without any white space, thus there is no need to place any additional dynamic RRH between these two vertices. Hence, in order to cover the whole circular coverage range of the static RRH, at least three and at most five dynamic RRHs are required. However, as the real coverage range of static RRHs may overlap, the required dynamic RRHs can be fewer than three. Fig. 2(b) illustrates the case of a pentagon in which the five dynamic RRHs can cover the serving area of the static RRH. However, when the number of sides of the Voronoi polygon becomes six or larger, as shown in Fig. 2(c), the maximum number of required dynamic RRHs to protect the static RRH is still five. For instance, the hexagon shown in Fig. 2(c) only required three dynamic RRHs to cover the serving area of static RRH.

### III. PROPOSED PROTECTION SWITCHING ARCHITECTURE

In the network architecture shown in Fig. 1, the remote node is passive and the optical receivers at the RRHs are colorless. In order to assure the availability of the static RRH network at off-peak times, the failed static RRH can be protected by activating the nearby dynamic RRHs which can cover the same serving area as the failed static RRH. A protection layer, as shown in Fig. 3(a), is added between the output ports of the AWG and the dynamic RRHs. When a certain static RRH is detected failed, its connected AWG port together with its protecting dynamic RRHs will be switched to the protection layer immediately. The set of protecting dynamic RRHs for each static RRH can be pre-assigned and the protection switching can be realized, via the network control plane.

As shown in Fig. 3(b), the protection layer consists of a number of optical switches and optical power splitters. The affected optical signal from the AWG first passes through an N-to-1 switch, where N corresponds to the number of the output ports of the AWG. As we have assumed at most one static RRH failure at any time, only one AWG port will be connected to the protection layer. Then, the optical signal is fed into a 1×5 optical switch. In section II, we have discussed the maximum number of required dynamic RRHs for protection of the static RRH is five. For a particular static RRH, as the protecting RRHs may not be as many as five, to avoid the unnecessary power loss, we set five different power splitting options, as illustrated in Fig. 3(b). Then, the split signals are fed into the switch network to route and connect to different groups of dynamic RRHs for protection. There are five groups because the maximum number of required protecting dynamic RRHs is five. The dynamic RRHs are divided into the five groups where in each group, the RRHs cannot serve the same static RRH. The number of RRHs in each group does not need to be the same.

As the target protecting dynamic RRHs can be in any subset of the five groups, we design a switch network, as shown in Fig. 3(c), to support all the possible connection combinations. In this way, the connections to the dynamic RRHs are reconfigurable. The label numbers at the inputs of the switch network indicate their corresponding connected power splitters. Thus, the switch network has fifteen inputs and five outputs. The number of switches required in this switch network has been optimized, such that only five 2×2 switches, and five 3×1 switches are required.

The proposed switch network can support all combinations. Fig. 4 shows the possible connection combinations of the switch network when four protecting dynamic RRHs are required, as an example to illustrate the operation. The dash
lines refer to the cases that either output can be chosen which leads to different results. The routing path is not unique because the power split partitions are identical. Fig. 5 shows the possible connection combinations of the switch network when five protecting dynamic RRHs are required.

Our proposed architecture of the protection layer has several significant advantages. First, the switch network is fully reconfigurable to broadcast the signal originally designated for the failed static RRH to the assigned set of dynamic RRHs, hence the mobile units in the serving area of the failed static RRH can still be connected to the central office. All protection switching patterns are pre-planned and stored in the network control plane, thus the incurred switching time can be very short and only depends on the physical switching time of the optical switches in the switch network. Moreover, the protection layer shows good scalability. As we have shown that at most five protecting dynamic RRHs are required for protection of one static RRH, even if more ports of the AWG or more RRHs are added to the network, we only need to modify the input $N$-to-1 switch and the output 1-to-$M$ switches while the core switch network can be kept unchanged. Besides, the modular design of the switches simplifies and optimizes the design of the switch network.

IV. SUMMARY

We have proposed a reconfigurable scheme for RRH protection in C-RAN systems. We have investigated the maximum number of required protecting dynamic RRHs and also designed a protection layer to support connection of the dynamic RRHs for static RRH protection. Our proposed system exhibits attractive features of connection re-configurability, scalability, and modular switch design.

REFERENCES


