Soft Handoff in CDMA and Wireless Security

During soft handoff, a mobile station is in the overlapping cell coverage area of two sectors belonging to two different base stations. The communications between mobile station and base station occur concurrently via two air interface channels from each base station separately. Both channels (signals) are received at the mobile station by maximal combining Rake processing (see Figure 11.20). Soft handoff occurs in about 20–40% of calls. Soft handoffs are an integral part of CDMA design. The determination of which pilots will be used in the soft handoff process has a direct impact on the quality of the call and the capacity of the system. Therefore, setting soft handoff parameters is a key element in the system design for CDMA. In the uplink direction, soft handoff differs signifi cantly from softer handoff: the code channel of the mobile station is received from both base stations, but the received data is routed to the base station controller (BSC) for combining. This is done so that the same frame reliability indicator as provided for outer loop power

control is used to select the better frame between two possible candidates within the BSC. A brief description of each type of pilot set is given below:

The ***active set*** is the set of pilots associated with downlink traffic channels assigned to the mobile units. The active set can contain more than one pilot because a total of three carriers, each with its own pilot, could be involved n a soft handoff process.

The ***candidate set*** consists of the pilots that the mobile unit has reported are of a sufficient signal strength to be used. The mobile unit also promotes the neighbor set and remaining set pilots that meet the criteria to the candidate set.

The ***neighbor set*** is the list of the pilots that are not currently on the active or candidate pilot lists. The neighbor set is identifi ed by the base station via the neighbor list and neighbor list update messages.

The ***remaining set*** contains all possible pilots in the system that can possibly be used by the mobile unit. However, the remaining set pilots that the subscriber unit looks for must be a multiple of Pilot_Inc. The parameters used to control the movement of a pilot from a neighbor to a candidate, to active, and then back to neighbor set are given below:

1. Pilot strength exceeds **T_ADD** and the mobile unit sends a pilot strengthmeasurement message (PSMM) and transfers the pilot to the candidateset.
2. The pilot strength drops below **T_DROP** and the mobile unit begins thehandoff drop time **(T_TDROP)**.
3. **T_COMP** is used into decision matrix for adding and removing pilots from the neighbor, candidate, and active set.

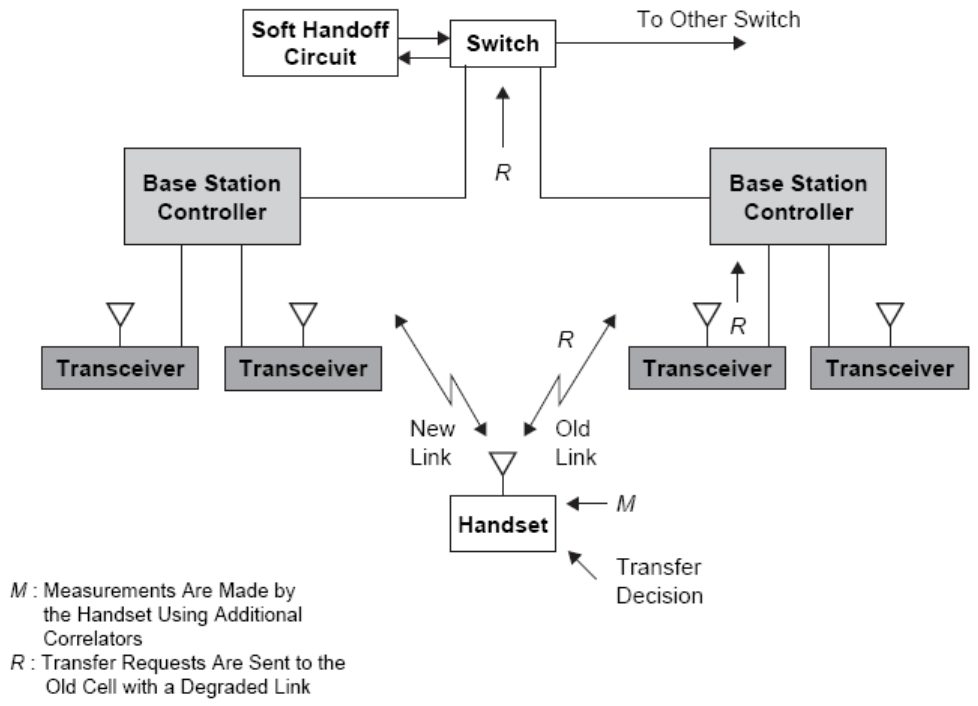

Figure 11.20 Soft handoff in CDMA.

Wireless security:

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks.

Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues [1]. Crackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into wired networks [2]. As a result, it's very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources.[3] Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.

The risks to users of wireless technology have increased as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Crackers had not yet had time to latch on to the new technology and wireless was not commonly found in the work place. However, there are a great number of security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level.[4] Cracking methods have become much more sophisticated and innovative with wireless. Cracking has also become much easier and more accessible with easy-to-use Windows or Linux-based tools being made available on the web at no charge.

Some organizations that have no wireless access points installed do not feel that they need to address wireless security concerns. In-Stat MDR and META Group have estimated that 95% of all corporate laptop computers that were planned to be purchased in 2005 were equipped with wireless. Issues can arise in a supposedly non-wireless organization when a wireless laptop is plugged into the corporate network. A cracker could sit out in the parking lot and gather info from it through laptops and/or other devices as handhelds, or even break in through this wireless card-equipped laptop and gain access to the wired network.

Source : http://nprcet.org/e content/Misc/e-Learning/ECE/IV year-VIII semester/EC1016 WIRELESS NETWORKS.pdf