

Communications Commission) i USA och använder sig av två olika tekniker beroende på överföringshastighet.

4.1. FHSS

Vid FHSS (Frequency Hopping Spread Spectrum) hoppar överföringen mellan olika frekvenser inom ett visst intervall enligt ett givet mönster.

Hoppen sker med högst 0,4 sekunders mellanrum och skillnaden mellan aktuell frekvens och nästa ska vara minst 6 MHz (i praktiken är hoppen större och sker med intervall om någon eller några hundradelar av en sekunds mellanrum).

Eftersom skillnaden är tillräckligt stor för att kanalerna inte ska störa varandra är denna metod robust och ger bra täckning, men överföringshastigheten är inte lika hög som när DSSS (se nedan) används.

Säkerheten i FHSS är god även om förbindelsen inte är krypterad. Eftersom sändningstiderna på enskilda kanaler oftast rör sig om några hundradelar av en sekund, kommer en avlyssnare som inte känner till frekvenshoppmönstret att höra något enstaka "blipp" som lika gärna kan vara en yttre störning.

4.2. DSSS

DSSS (Direct-Sequence Spread Spectrum) använder sig som tidigare nämnts av samma frekvensband som FHSS, men med den stora skillnaden att frekvenserna inte ändras. Istället delas frekvensområdet upp i tre kanaler som vardera kommunicerar på 11 Mbit/s, vilket är snabbare och mindre effektkrävande än FHSS. Nackdelen är ökad störningskänslighet och kortare kommunikationsavstånd. DSSS är den teknik som ingår i standarden 802.11b.

5. Säkerhet

Kommunikation enligt 802.11 krypteras alltid, oavsett om FHSS eller DSSS används. Metoderna för detta använder nycklar om 40, 64 eller 128 bitar. Eftersom radiovågor kan "läcka" från ett rum eller byggnad kan de lättare avlyssnas och därför är det viktigt att kryptera trådlösa förbindelser.