



MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
DE SANTA CATARINA
CAMPUS SÃO JOSÉ
Curso de Engenharia de Telecomunicações

Aspectos de Segurança na camada PHY: DSSS, FHSS e OFDM

Henrique Hilleshein
Lucas Thiesen
Mathias Hillesheim

São José, Julho de 2016

As **redes locais** utilizam ondas rádios ou infravermelhas para transmitir dados. *A técnica utilizada no início para as transmissões rádios chama-se transmissão em banda estreita, consiste em passar as diferentes comunicações em canais diferentes* (KIOSKEA, 2014). Porém, as transmissões rádios têm numerosos problemas que tornam este tipo de transmissão insuficiente, como por exemplo a divisão da banda concorrida entre as diferentes estações presentes numa mesma célula ou a propagação por caminhos múltiplos de uma onda rádio. Para contornar esses problemas, a camada física da norma 802.11 define várias técnicas de transmissão que permitem limitar os problemas devidos às interferências como a técnica de espectro com salto de frequência, a técnica de espectro de sequência direta, e alguns tipos de modulação. Nesse resumo estarão apresentadas três dessas técnicas utilizadas.

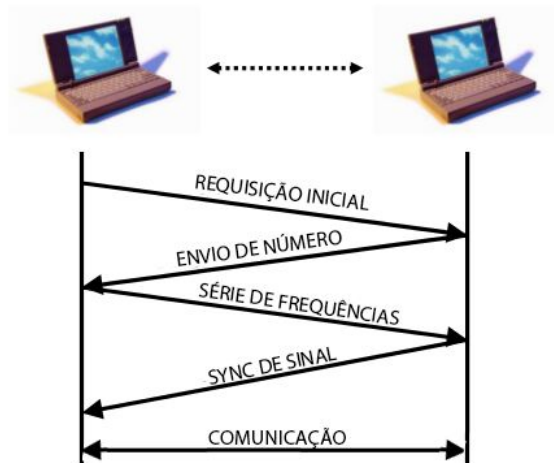
O **DSSS (*Direct Sequence Spread Spectrum*)**, ou sequência direta de espalhamento do espectro é uma modulação que separa uniformemente a largura de banda em uma série de canais, e ao transmitir troca de canal sequencialmente. A ideia do DSSS é espalhar os quadros por toda a sua largura de banda com uma sequência de bits, chamado de chip, que é basicamente um código. Ele pode possuir valor 1 ou -1 e é modulado de acordo com sinal de informação. Como esse código é espalhado por toda a largura de banda ele é chamado de pseudo-ruído (PN). Graças a esse pseudo-ruído, quem enxerga o sinal de fora o enxerga como um ruído, aumentando a imunidade com interferências.

A segurança do DSSS se baseia no próprio chip, onde só o receptor que possui essa informação consegue decodificar o sinal. Se utilizando um método matemático, onde se multiplica o chip pelo sinal recebido e caso o chip esteja correto o receptor conseguirá decodificar o sinal de informação. Esse é o grande gerador de segurança, pois para todos os outros receptores aquela conversação aparenta ser um ruído.

FHSS (*Frequency-hopping spread spectrum*) é um método de transmissão de sinais de rádio que consiste na mudança constante da portadora através de vários canais de frequência, usando uma sequência pseudo-aleatória conhecida por ambos transmissor e receptor.

Uma transmissão de espectro variável apresenta várias vantagens relacionadas a sua aplicação, e uma das principais diz respeito a sua segurança. Devido ao jeito que o FHSS

funciona, fica muito difícil a prática de técnicas como o jamming (interceptação de sinal). O início de uma comunicação que implementa o FHSS se dá da seguinte maneira:



onde no segundo passo da comunicação, ocorre a geração de um número randômico que é utilizado em um algoritmo para se calcular uma série de frequências. Essas frequências ficam definidas como as que serão usadas como canais de comunicação pela portadora. Dessa maneira, a interceptação do sinal fica muito difícil, sendo que somente os participantes da comunicação saberão a frequência que a portadora utilizara para transitar, lembrando que essa frequência é alterada constantemente durante a comunicação.

Esse aspecto de segurança da tecnologia FHSS faz com que ela seja usada até mesmo com objetivos militares. Rádios militares utilizam técnicas criptográficas para gerarem as faixas de frequência onde a portadora irá circular. Dessa forma, a comunicação assume altos níveis de segurança, sendo que o uso de criptografia aliada a implementação do FHSS torna praticamente inviável o jamming na comunicação.

O **OFDM** (*orthogonal frequency division modulation/multiplexing*) opera utilizando vários canais baseando-se em uma técnica parecida com FDM onde ele separa os canais por frequências ortogonais e divide o espectro em um total de 52 canais sendo 4 canais destinados para controle e os outros 48 para dados. Existe ainda uma variação mais complexa e também mais utilizada: o COFDM, que além de fazer a separação por frequências ortogonais, também gera códigos nas transmissões para melhorar as taxas de transferência e confiabilidade dos dados.

O OFDM/COFDM é considerado um método extremamente eficiente pois separa os dados em várias partes e faz uma espécie de transmissão em paralelo. Dessa forma, ele multiplica a taxa de transmissão e cria um grande espalhamento de espectro, que garante um ótimo desempenho ao evitar ruídos e interferências.

Um importante aspecto de segurança do OFDM/COFDM é a sua capacidade de separar sua informação em várias subportadoras e detectar anomalias nessas subportadoras podendo isolar e trocar as faixas de frequência usadas de acordo com a necessidade, caso alguém mau intencionado tente acesso ao canal e cause algum tipo de alteração (interferência, ruído ou outro fenômeno que altere a qualidade ou confiabilidade do sinal) pode fazer com que o OFDM isole a subportadora anômala ou até redefinir suas faixas de frequência para garantir maior confiabilidade à informação.

CONCLUSÃO

Fazendo uma **rápida comparação** entre as três tecnologias, consegue-se perceber que não existe necessariamente uma melhor que a outra. Entre eles, o FHSS é o que oferece uma maior segurança, se valendo do seu método de transmissão onde ele muda a faixa de frequência que a portadora transita através de saltos, que acontecem aproximadamente a cada dois quadros transmitidos. Tais frequências são conhecidas apenas pelas partes que participam da comunicação. Aliado a tecnologias de encriptação, essa opção é escolhida até por corporações militares. Apesar da sua segurança, todavia, não é a tecnologia mais otimizada, levando-se em conta que utiliza uma banda grande, que não é totalmente utilizada durante toda a transmissão. Esse é o mesmo problema do DSSS. Essa tecnologia, por sua vez, por mais que seja bem parecida com o próprio FHSS (ambas se baseiam no espalhamento de espectro e possuem taxas de 1Mbps a 2Mbps), tem suas particularidades. Também utilizado amplamente no meio militar, essa tecnologia utiliza uma grande faixa de frequência para fazer sua transmissão, sendo esse um dos seus pontos negativos. Porém, assim como o seu parente próximo, o FHSS, ele garante grande segurança de transmissão, contando que você consiga proteger o seu *chip*. Enquanto o FHSS é mais robusto e menos sensível ao meio (ruídos, colisões, reflexões), o DSSS possui uma maior capacidade. O OFDM, por sua vez, traz um aspecto contrário. Como ele pega uma faixa de frequência e divide ela em várias faixas ortogonais, ele de fato utiliza toda a faixa que foi alocada para ela. Assim, ele acaba melhorando o throughput da transmissão, mesmo não possuindo todos os aspectos avançados de segurança que o DSSS e o FHSS possuem. Assim, pode-se concluir que cada um se destacará para determinada aplicação. Quando você não necessita de uma segurança maior e deseja um throughput maior, o OFDM se mostra mais atraente. Se você deseja segurança, e densidade espectral de potência muito baixa, o DSSS ou o FHSS seria uma melhor escolha.

REFERÊNCIA

- KIOSKEA. **As técnicas de transmissão de dados nas redes sem fios Wi-Fi (80.** Kioskea.net, 2014. Disponível em: <<http://br.ccm.net/contents/795-as-tecnicas-de-transmissao-de-dados-nas-redes-sem-fios-wi-fi-80>>. Acessado em: 25 jul 2016.