MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA
ENGENHARIA DE TELECOMUNICAÇÕES
CAMPUS SÃO JOSÉ

Aspectos de Segurança do padrão IEEE802.11ac

Alunas: Alline Silva Domingos, Jessica da S. Hahn e Layssa Alves Pacheco.

INTRODUÇÃO

A segurança da informação é um ponto de extrema importância dentro dos meios de comunicações. Manter a segurança dos dados que circulam por um rede não é tarefa fácil, já que a vulnerabilidade a ataques sempre existirá dentro de uma rede, seja ela cabeada ou sem fio. Em redes sem fios estabelecer um mecanismo que possa garantir sua segurança é um grande desafio para um administrador de redes, pois diferente das redes cabeadas as redes wireless no padrão IEEE 802.11 emitem um sinais de radiofrequência para que todos seus clientes possam “ouvi-lá”. Entretanto qualquer aparelho com capacidade de captura, consegue detectá-lo caso esteja dentro de seu alcance. Desta forma, uma rede sem fio não somente deve se proteger do acesso não autorizado, como fazem as rede cabeadas, mas também de usuários que conseguem se conectar a ela, mas não deveriam. E devido a isto os padrões da norma IEEE 802.11 vem passando por melhorias em aspecto de desempenho e de mecanismo de segurança para garantir um bom funcionamento das rede wifi. A quinta geração com a norma 802.11ac que ainda está em processo de elaboração adota algumas destas melhorarias.

1.0 O padrão IEEE802.11ac

No fim do século passado iniciou-se os trabalhos referentes as redes sem fio, o padrão 802.11. De acordo com as necessidades surgiram padrões baseados nos princípios da 802.11, porém aperfeiçoados em determinados aspectos. A mais recentes é a 802.11ac, publicada em Dezembro de 2013, criada para operar em faixa de frequência de 5GHz com o intuito de diminuir problemas de interferências existentes em rede wi-fi. O padrão 802.11ac surgiu com alterações ao nível físico e de controle de acesso ao meio permitindo um aumento significativo na velocidade de transmissão de dados para a utilização de múltiplos dispositivos com requisitos de largura de banda e latência elevados, assim com aumento no número de usuários por ponto de acesso (AP, acess point) e a melhoria na experiência de cada com o a rede wifi, provenientes do avanço tecnológico sofrido pelo meio de transmissão e equipamentos aos passar dos anos.

1.1 Diferenciais entre os demais padrões 802.11

As principais diferenças entre o padrão 802.11ac e os anteriores são:

- Alta velocidade de transmissão, enquanto os outros padrões trabalham com velocidades inferiores, o 802.11ac suportar velocidades de transmissão de dados de superiores a 1 Gbps para multi estações ou de 500 Mbps para uma estação.
- Alta frequência de operação de 5 GHz, enquanto os demais padrões operam entre 2,4GHz;
- Utilização de modulação 256 QAM;
- Aumento no número de canais suportados na tecnologia MIMO, dos 4 canais máximos no 802.11n o padrão 802.11ac passa para o suporte de 8 canais;
- Utilização de canais de 80 MHZ ou 160 MHz;
- Alcance, podendo se comunicar com estações que estejam a 200 metros de distância (Figura 1.1-a);
- Beamforming, capacidade de transmissão direcional para regiões onda há dispositivos conectados aos roteadores que operam neste padrão (Figura 1.1-b).

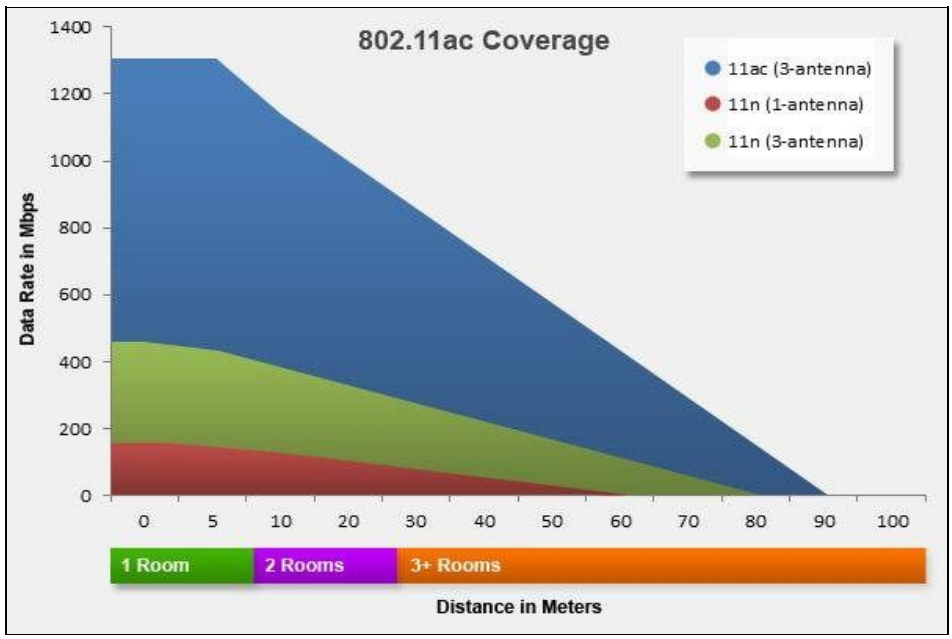

Figura 1.1- a : Alcance dos padrões 802.11[1]

Apesar das alterações a nível físico e de controle de acesso ao meio (MAC) o padrão 802.11ac mantem compatibilidade com normas IEEE 802.11 anteriores na banda do 5 GHz.

[1] Retirado do site http://www.hardware.com.br/artigos/entendendo-wifi-802.11-ac/

Figura 1.1 - b: Beamforming[2]

2.0 Segurança

2.1 Tipos de ataques a redes sem fio

Um dos grandes problemas de segurança das redes sem fio é a falta de controle sobre o meio de transmissão, por se tratar de um meio que utiliza ondas eletromagnéticas qualquer pessoa pode acessar o meio, por este motivo a segurança nas redes sem fio se baseia em criptografia dos dados, controle de acesso por senhas, SSIDs, entre outros. Os ataques a esse tipo de rede podem ser classificados da seguinte maneira:

- Ataques a criptografia e autentificação - onde o invasor consegue “quebrar” a criptografia e a senha de autentificação da rede;
- Ataques a negação de serviço - referente a clonagem de um endereço MAC pertencente a uma determinada rede sem fio;
- Ataques a falsificação de APs - um AP falso é inserido ou mascarado na rede roubando as informações das estações conectadas a ele (Figura 2.1-a);

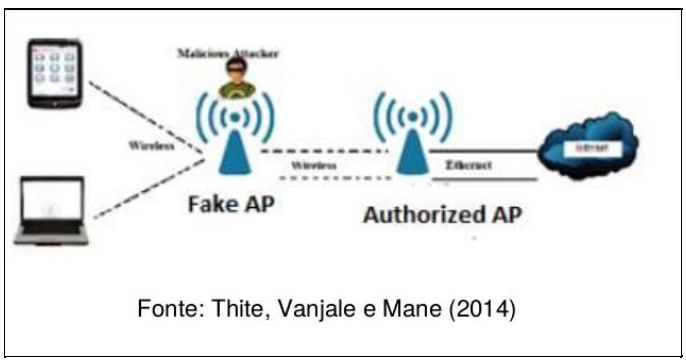

Figura 2.1-a: Falsificação de um AP

[2] Retirado do site http://blog.dlink.com/wireless-router-buying-guide/

2.2 Segurança do padrão 802.11ac

Como já dito anteriormente o grande motivo para a criação deste padrão foi o aumento da velocidade e a melhora do acesso ao meio. Porém, a criação do padrão também se preocupou com a segurança do usuário, devido a expansão e a velocidade de crescimento do rede, mesmo que esse não fosse o foco do padrão. Com isso, houveram alterações nas especificações para estabelecer o *Robust Security Network Association* (RSNA), que são redes que apresentam melhoras referentes as falhas já conhecidas do WEP, no *Distribution System* (DS) definindo um conjunto de caraterísticas de segurança além do *Wired Equivalente Privacy* (WEP) e a autenticação IEEE802.11, que consiste na primeira etapa na conexão de rede para estabelecer a identidade com um ponto de acesso ou roteador sem fio de banda larga (nenhuma criptografia de dados ou segurança está disponível nesse estágio). Esses recursos incluem os seguintes:

- Mecanismos de autenticação reforçada para STA;
- Algoritmos de gestão de chaves;
- Estabelecimento de chaves criptográficas;
- Reforço nos mecanismos de encapsulamento criptográfico de dados, tais como: Counter modewith Cipher-block chaining Message authentication code Protocol (CCMP), Galois CounterMode Protocol (GCMP) e Temporal Key Integrity Protocol (TKIP);
- Mecanismo rápido de transição de BSS.

Além disso o padrão 802.11ac opera com os seguintes padrões de segurança já implantado em outras versões, como:

- WEP (Wired Equivalent Privacy):
  O Protocolo WEP lançado em 1997, como padrão de segurança de rede sem fio utiliza como mecanismo de proteção algoritmo criptografia RC4 (*Ron's Cipher 4*) que codifica a mensagem carácter a carácter, por meio de uma sequencia de *Keystream* gerando uma chave inicial. Com isso, o mecanismo busca cumprir algumas metas de segurança:
  a) Autenticação(Controle de acesso) - Garantir que somente pessoas autorizadas terão acesso a rede.
  b) Criptografia(Confiabilidade) - deve evitar que intrusos compreendam o trafego capturado.
  c) Integridade da informação - deve garantir que dados trocados não sofram alterações por intrusos.

  Entretanto, por utilizar como base um algoritmo não muito robusto, o protocolo não consegue garantir a segurança da rede, tornando-se vulnerável devido a facilidade de "quebra" de criptografia existente no algoritmo RC4.
- WPA (Wifi Protected Acess)/WPA2 (Wifi Protected Acess 2): surgiu com a necessidade de suprir as fragilidades do WEP, com um vetor de inicialização chave

criptográfica de 48 bits, chave temporal (TKIP) e mecanismo de atualização de chaves.

- WPA-PSK (Pre-Shared Key)/WPA2-PSK (Pre-Shared Key 2): o WPA é dividido de acordo com seu uso: WPA para uso pessoal (usuários comuns) e o WPA para uso empresarial, de acordo com o tipo de uso o WPA possui chaves diferentes, no caso do uso pessoal seria utilizado o WPA-PSK com as especificações citadas no WPA/WPA2.
- MAC Adress Filtering: utilizado nos roteadores sem fio, opção que permite que o administrador da rede configure manualmente os endereços MAC que o roteador irá aceitar a conexão, ou seja, o roteador está limitado a aceitar conexões apenas dos endereços cadastrados.

	Autentificação	**Distribuição de chaves**	**Alteração de chaves**	**Criptografia**
WEP	Chave WEP	Manual	Fixo	RC4
WPA	802.1x, EAP	Automático	Dinâmico	RC4
WPA2	802.1x, EAP	Automático	Dinâmico	AES-CCMP

Tabela 2.2.0 - Diferenças entre os padrões WEP,WPA/WPA2

REFERÊNCIAS

CISCO SYSTEMS. **802.11ac: The Fifth Generation of Wi-Fi Technical White Paper**. Disponível em: <Inc.http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-3600-series/white_paper_c11-713103.html>. Acesso em: 25 jul. 2016.

SERENO; José Humberto Laranjeira. **Tendências de implementação e segurança nas redes wireless organizacionais.** 106 p. 2015. Dissertação (Mestrado em Sistemas de Informação Organizacionais) - Escola Superior de Ciências Empresariais, Instituto Politécnico de Setúbal, Portugal, 2015.

FIGUEIREDO; Davis Anderson. **A análise da segurança de redes wi-fi através de teste de penetração em instituições de ensino superior de Belo Horizonte.** 39 p. 2015. Artigo de requisito parcial para título de Mestre (Mestrado Profissional em Sistemas de Informação e Gestão do Conhecimento) - Universidade FUMEC, Belo Horizonte, 2015.

CAÇADOR; Daniel Maximino. **Segurança e Mobilidade em Redes IEEE 802.11:** Modelo de suporte à decisão na escolha de arquitecturas e tecnologias de redes sem fios. Dissertação (Mestre em Segurança em Sistemas de Informação) - Faculdade de Engenharia, Universidade Católica Portuguesa, Portugal, 2014.

MOHAMMED; Farik, ABM; Shawkat Ali. Recurrent Security Gaps In 802.11ac Routers. **International Journal of Scientific & Technology Research,** v. 4, n. 9, 2015.

Aspectos e mecanismos de segurança no padrão IEEE 802.11. Disponível em: <http://www.maxwell.vrac.puc-rio.br/7589/7589_4.PDF>. Acesso em: 25 jul. 2016.

WEP, WPA/WPA2. Disponível em: <http://wep-wpa-or-wpa2-1307.hargaponsel.info/>. Acesso em: 25 jul. 2016.

Wi-fi security. Disponível em: <http://pt.slideshare.net/veeru3112/wi-fi-security-34019886>. Acesso em: 25 jul. 2016.