REDES SEM FIO

MOBILIDADE EM REDES SEM FIO

Autor: Me. Ubiratan Roberte Cardoso Passos
Revisor: Rogério de Campos

INICIAR

introdução

Introdução

Duas importantes questões relacionadas às redes sem fio estão relacionadas à sua segurança, devido principalmente pela sua abrangência e abertura de sinal, que é fácil de ser gerado e também capturado por qualquer dispositivo com receptor de sinal de rádio, e mobilidade dos dispositivos, que vai muito além da possibilidade de transitar com o dispositivo dentro de uma mesma rede, pois permite que estes migrem de uma rede para outra de forma totalmente transparente para os usuários e aplicações.

Durante os estudos, questões relacionadas a mobilidade em redes sem fio, equipamentos, mobilidade em uma mesma sub-rede IP, nomadicidade, taxas de transmissão ajustáveis, gestão de energia e segurança em redes sem fio serão abordadas.

Mobilidade em Redes sem Fio

Mobilidade em redes sem fio, assim como o próprio conceito de mobilidade, pode levar a diversos entendimentos. Em termos de redes sem fio, não se pode limitar a ideia de mobilidade ao simples fato de ser possível acessar a rede de qualquer ponto dentro do limite do alcance desta rede.

Conceitos de Mobilidade em Redes sem Fio

Segundo Engst e Fleishman (2005), o conceito de mobilidade em redes sem fio envolve questões muitas vezes não tão simples, tais como: questões físicas, estruturais e também diversos algoritmos que tornem a arquitetura da rede capaz de permitir que o dispositivo se conecte ou se mantenha conectado mesmo que não esteja sempre conectado à mesma rede.

Redes Móveis e Redes sem Fio

Primeiramente é preciso deixar clara a distinção entre **redes sem fio** e **redes móveis** . As **redes sem fio** são dispositivos que se conectam através de **enlaces** sem fio. Já as **redes móveis** , por sua vez, estão relacionadas ao

roteamento dos dispositivos/usuários móveis que, frequentemente, mudam seu ponto de entrada/ligação (não somente físico) na rede.

Figura 2.1 - Correntes de conexão
Fonte: Aimage / 123RF.

De acordo com Tanenbaum e Wetherall (2011), mobilidade em redes sem fio é, ao mesmo passo que, algo muito diferente de conexão em redes sem fio, dependente da tecnologia de conexão sem fio. Mobilidade em redes sem fio está relacionada com a capacidade de o dispositivo mudar de uma rede para a outra com total transparência para o usuário, com todo controle de endereçamento de IP, recursos de segurança e conectividade realizados diretamente pelos dispositivos sem a necessidade de qualquer interferência do usuário.

Para entender o que vem a ser mobilidade em redes sem fio, deve-se entender o termo **nomacidade** . De forma básica, o termo por ser entendido como a capacidade de os dispositivos que possuem atributos de mobilidade, comportam-se como nômades, podendo migrar entre as diversas redes sem fio existentes sem qualquer problema.

Dispositivos Estáticos, Portáteis e Móveis

Seja em redes com fio, sem fio ou redes móveis, pode-se classificar os dispositivos que são utilizados para fornecer e receber os sinais em três grupos, são eles:

- **Dispositivos estáticos** : não apresentam qualquer característica de portabilidade ou mobilidade. Uma vez inseridos em algum ambiente, ou seja, uma vez que seu posicionamento é definido, dificilmente sofrerá alguma movimentação. Esses dispositivos não foram preparados para serem transportados, a não ser que sejam desligados e por vezes desmontados. Configurar o acesso à rede para esses dispositivos tende a ser menos complexo do que para dispositivos portáteis ou móveis.
- **Dispositivos portáteis** : podem, em muitos casos, ter características (de hardware) semelhantes às dos dispositivos estáticos, exceto por um detalhe muito importante: esses dispositivos são adaptados para a portabilidade, ou seja, podem ser movidos de um ambiente para o outro com facilidade, não sendo preciso ser desligado. São exemplos: notebooks, tablets etc.
- **Dispositivos móveis** : em certos momentos, confundem-se com os dispositivos portáteis. Nem todo dispositivo portátil é móvel, assim como não se pode afirmar que todo dispositivo móvel é portátil. Até mesmo alguns veículos podem ser móveis (no sentido de conectividade), mas não são portáteis. Deve-se entender um dispositivo como móvel por sua capacidade de migrar ou acessar diferentes enlaces de conexão de forma totalmente transparente para o usuário.

É importante que não haja confusão, sobretudo sobre dispositivos portáteis e dispositivos móveis, já que o fato de poder mover o dispositivo com facilidade desperta a impressão de mobilidade. O termo mobilidade no âmbito de redes sem fio refere-se ao fato de as camadas de acesso à rede serem capazes de contemplar a existência de dispositivos que se conectam de diversos pontos (geograficamente distantes e, por vezes, em sub-redes diferentes) à sua rede de origem.

Mobilidade na Mesma Sub-rede IP

Para que a mobilidade dos usuários seja totalmente transparente para os aplicativos de rede, os dispositivos que acessam a rede devem manter seu endereço enquanto se movimentam de uma rede para outra.

Quando um nó móvel é residente em uma rede estrangeira, todo o tráfego endereçado ao endereço permanente do nó agora precisa ser roteado para a rede estrangeira. Como isso pode ser feito? Uma opção é a rede estrangeira anunciar para todas as outras redes que o nó móvel reside em sua rede. Isso poderia evitar a troca usual de informações de roteamento entre domínios e exigiria poucas alterações na infraestrutura de roteamento existente. Quando o nó móvel sai de uma rede externa e se une à outra, a nova rede externa anuncia uma nova rota altamente específica para o nó móvel, e a antiga rede estrangeira retira suas informações de roteamento em relação ao nó móvel.

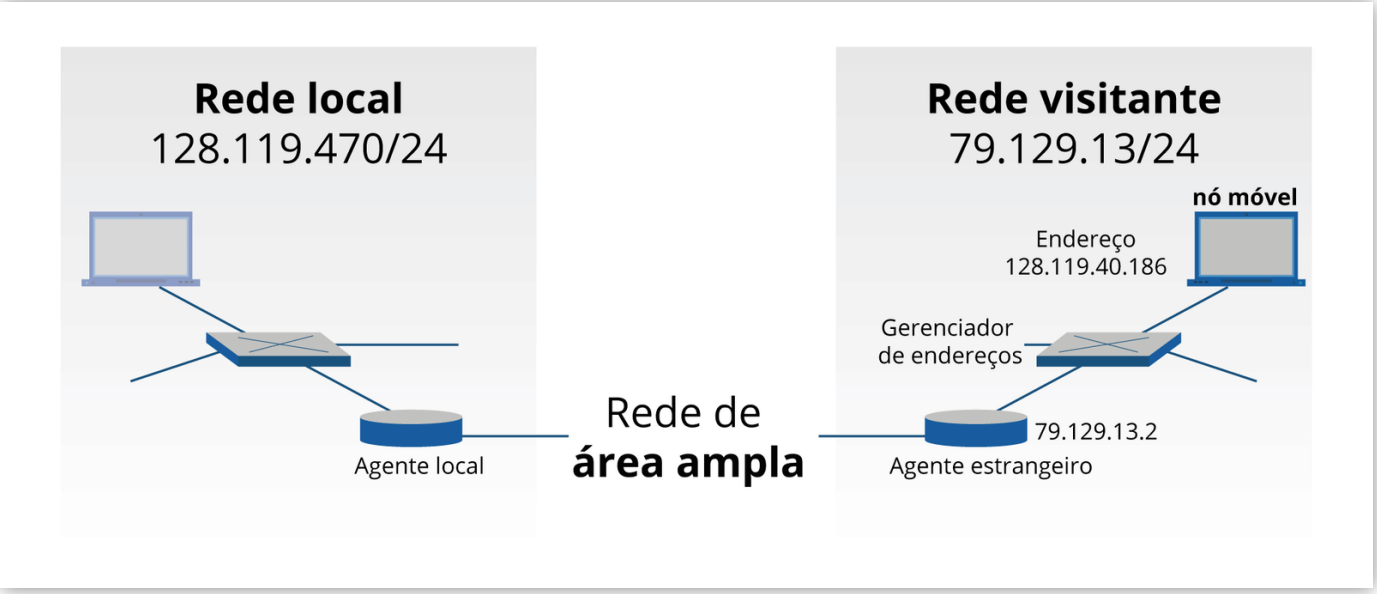


Figura 2.2 - Mobilidade em redes sem fio
Fonte: Adaptado de Rochol (2018, p. 558).

Com isso dois problemas são resolvidos simultaneamente, sem a necessidade de alterações significativas na infraestrutura da camada de rede. Outras redes conhecem a localização do nó móvel e é fácil rotear **datagramas** para o nó móvel, pois as tabelas anteriores direcionam os **datagramas** para a rede externa.

saiba mais

Saiba mais

Assim como no modelo de referência OSI, no modelo TCP/IP a camada de transporte é responsável por transmitir os dados de um dispositivo para o outro, independentemente do tipo de tecnologia utilizada, ou seja, seu dever é garantir a existência de comunicação entre os dispositivos de origem e destino do pacote. A camada de transporte possui dois protocolos de comunicação bastante populares, são eles: TCP (Transmission Control Protocol) e o UDP (User Datagram Protocol).

ACESSAR

Uma desvantagem significativa, no entanto, é a escalabilidade. Se o gerenciamento de mobilidade fosse responsabilidade dos roteadores de rede, os roteadores teriam que manter as entradas da tabela de encaminhamento para milhões de nós móveis e atualizá-las à medida que os nós se movem.

Uma abordagem alternativa (adotada na prática) é a funcionalidade da mobilidade por ***push*** do núcleo da rede até a borda da rede. Nesse modelo, o agente local pode rastrear a localização dos seus nós móveis até as redes visitantes na qual se encontram. No caso, um protocolo entre o nó móvel (ou um agente estrangeiro que representa o nó móvel) e o agente doméstico, certamente será necessário para atualizar a localização do nó móvel.

Uma função do agente estrangeiro é criar um chamado endereço de atendimento (COA) para o nó móvel, com a parte da rede do COA correspondente à da rede externa. Portanto, existem dois endereços associados a um nó móvel, seu endereço permanente (análogo ao endereço residencial de um indivíduo) e seu COA, às vezes conhecido como endereço estrangeiro (análogo ao endereço da casa na qual o indivíduo está residindo

no momento). Uma segunda função do agente estrangeiro é informar ao agente doméstico que o nó móvel reside na sua rede (do agente estrangeiro) e possui o COA fornecido.

praticar

Vamos Praticar

Mobilidade em redes sem fio vai muito além da capacidade de transitar com um dispositivo (portátil ou não) de um ponto para o outro, conectando-se às diferentes redes sem fio, cada uma com suas regras e características, criando regras para transmissão de dados a cada nova rede à qual o dispositivo for conectado. Dessa forma pergunta-se: qual das respostas a seguir corresponde corretamente às regras de mobilidade em sub-redes de mesmo IP?

- **a)** Ao se locomover para outra rede, o dispositivo recebe um novo endereço de identificação, ao receber esse novo endereço de identificação novos protocolos de comunicação são estabelecidos para o dispositivo.
- **b)** Ao se locomover para outra rede, a nova rede anuncia uma rota altamente específica para o nó móvel, e a antiga rede estrangeira retira suas informações do roteamento em relação ao nó móvel.
- **c)** Ao se locomover para outra rede, a nova rede externa determina a nova rota altamente específica para o nó móvel, e a antiga rede estrangeira retira suas informações de roteamento em relação ao nó móvel.
- **d)** Quando o nó móvel sai de uma rede externa e se une a outra, a nova rede local específica para o nó é criada, e uma nova rota altamente específica para a nova rede, e a antiga rede estrangeira retira suas informações de roteamento em relação ao nó móvel.

- **e)** Quando o nó móvel sai de uma rede externa e se une a outra, a nova rede externa anuncia uma nova estrutura de comunicação com novos protocolos e camadas de dados altamente específica para o nó móvel, e a antiga rede estrangeira retira suas informações de roteamento em relação ao nó móvel.

Segurança e Recursos Avançados do Padrão 802.11

Os padrões 802.11 foram desenvolvidos especificamente para definir a arquitetura a ser aplicada nos dispositivos de redes sem fio. Parte dessa arquitetura mantém as mesmas características de uma rede cabeada, entretanto, diversos novos recursos foram adicionados a fim de tornar os dispositivos mais adaptáveis e seguros.

Alguns dos recursos avançados relacionados ao padrão 802.11 que se destacam são: **capacidade de gerenciar/modificar a taxa de transferência de dados** , **capacidade de gerenciamento de energia do dispositivo** e **recursos de criptografia e segurança** .

Ajuste Automático de Taxa de Transmissão

Diferentes técnicas de modulação (com as diferentes taxas de transmissão) são apropriadas para diferentes cenários. Considere, por exemplo, um usuário móvel 802.11 que esteja inicialmente a 20 metros da estação base, com uma alta relação sinal / ruído (SNR). Nesse caso, o usuário pode se comunicar com a estação base usando uma técnica de modulação da camada

física que fornece altas taxas de transmissão enquanto baixas regras de codificação (BER).

Suponha agora que o usuário se torne móvel, afastando-se da estação base, com o SNR caindo à medida que a distância da estação base aumenta. Nesse caso, se a técnica de modulação usada no protocolo 802.11 que opera entre a estação base e o usuário não mudar, o BER se tornará inaceitavelmente alto à medida que o SNR diminuir e, eventualmente, nenhum quadro transmitido será recebido corretamente.

Por esse motivo, algumas implementações do 802.11 possuem a capacidade de adaptação de taxa que seleciona adaptativamente a técnica de modulação da camada física subjacente a ser usada com base nas características atuais ou recentes do canal.

Se um nó envia dois quadros a seguir sem receber uma confirmação (uma indicação implícita de erros de bit no canal), a taxa de transmissão volta para a próxima taxa mais baixa. Se forem confirmados 10 quadros a seguir, ou se um timer que acompanhar o tempo desde o último feedback expirar, a taxa de transmissão aumentará para a próxima taxa mais alta. Esse mecanismo de adaptação da taxa compartilha a mesma filosofia de "sondagem" do mecanismo de controle de congestionamento da TCP - quando as condições são boas (refletidas pelos recibos de ACK), a taxa de transmissão é aumentada até que algo "ruim" aconteça (a falta de recibos de ACK); quando algo "ruim" acontece, a taxa de transmissão é reduzida.

A adaptação da taxa 802.11 e o controle de congestionamento de TCP são, portanto, semelhantes à criança que constantemente pressiona seus pais por mais e mais até que os pais finalmente digam "chega”, e os filhos se afastam (apenas para tentar mais tarde, depois que as condições melhorarem!).

Gerenciamento de Energia

A energia é um recurso precioso em dispositivos móveis e, portanto, o padrão 802.11 fornece recursos de gerenciamento de energia que permitem que os

nós 802.11 minimizem a quantidade de tempo em que suas funções de detecção, transmissão e recebimento e outros circuitos precisam estar ativados, a gerência opera da seguinte maneira:

Um nó é capaz de alternar explicitamente entre os estados de suspensão e de vigília. Um nó indica ao ponto de acesso que ele entrará em suspensão configurando o bit de gerenciamento de energia no cabeçalho de um quadro 802.11 como 1. Um temporizador no modo ***then*** é então configurado para ativar o nó imediatamente antes do AP ser agendado para enviar seu quadro ***beacon*** (lembre-se de que um AP normalmente envia um quadro ***beacon*** a cada 100 ms).

Desde que o AP sabe pelo bit de transmissão de energia definido que o nó está inativo, ele (o AP) sabe que não deve enviar nenhum quadro para esse nó e armazenará em buffer os quadros destinados ao host adormecido para transmissão posterior. Um nó é ativado antes do AP enviar um quadro de sinalizador e, rapidamente, entra no estado totalmente ativo. Essa ativação requer apenas 250 microssegundos.

Os quadros de ***beacon*** enviados pelo AP contêm uma lista de nós, cujos quadros foram armazenados em buffer no AP. Se não houver quadros em buffer para o nó, ele poderá retornar ao modo de suspensão. Caso contrário, o nó pode explicitamente solicitar que os quadros em buffer sejam enviados, enviando uma mensagem de pesquisa para o AP.

Com um tempo entre ***beacon*** de 100 ms, um tempo de ativação de 250 microssegundos, é um tempo igualmente pequeno para receber um quadro ***beacon*** e verificar se não há buffer quadros, um nó que não possui quadros para enviar ou receber pode ficar adormecido 99% do tempo, resultando em uma economia significativa de energia.

Segurança em Redes sem Fio

A segurança é uma preocupação particularmente importante em redes sem fio, onde o dispositivo de transporte de ondas de rádio pode emitir ondas que

se propagam muito além do prédio que contém a estação base e os hosts sem fio.

Em redes do tipo sem fio, qualquer dispositivo ao alcance da rede pode enviar ou receber ondas (sinais) para essa rede. Dessa forma é fundamental que diversos parâmetros relacionados à segurança da informação sejam implementados.

reflita

Reflita

Uma das mais conhecidas características das redes sem fio está relacionada à abertura de seus sinais. Qualquer dispositivo que esteja ao alcance do gerador de sinais é capaz de captar tais sinais, assim como qualquer dispositivo próximo o suficiente pode enviar sinais para a rede. Sendo assim, como proteger a rede dos invasores, ou prevenir os equipamentos de receberem ou enviarem sinais de (ou para) dispositivos não interessados nos dados? Parte dessas soluções envolve criptografia de dados, e assinaturas dos pacotes que transitam pela rede.

Fonte: Soares e Moraes (2019).

Dos parâmetros relacionados à segurança da informação, dois são extremamente importantes para implementação da segurança em redes sem fio, o primeiro deles é a criptografia dos dados, onde os dados são convertidos em uma sequência alfanumérica quase indecifrável de caracteres; o segundo é a autenticidade do emissor, ou seja, trata-se de um mecanismo que permita identificar quem de fato é o emissor da mensagem.

Com esses recursos implementados em associação com outros que serão analisados a seguir, é possível aumentar significativamente a segurança em sistemas de redes sem fio.

praticar

Vamos Praticar

Diferentes técnicas de modulação (com as diferentes taxas de transmissão) são apropriadas para diferentes cenários. Caso um usuário se comunique com a estação base usando uma técnica de modulação da camada física pode haver altas taxas de transmissão e baixas regras de codificação, quando esse usuário está próximo da base. Entretanto, na medida em que este usuário se afasta da estação base, o SNR cairá à medida que a distância da estação base aumenta. Nesse caso, se a técnica de modulação usada no protocolo 802.11 que opera entre a estação base e o usuário não mudar, o BER se tornará inaceitavelmente alto à medida que o SNR diminuir e, eventualmente, nenhum quadro transmitido será recebido corretamente. Qual das opções abaixo descreve a técnica que impede que esse problema ocorra?

- **a)** Se um nó envia dois quadros a seguir sem receber uma confirmação (uma indicação implícita de erros de bit no canal), a taxa de transmissão volta para a próxima taxa mais alta. Se forem confirmados 10 quadros a seguir, ou se um timer que acompanhar o tempo desde o último feedback expirar, a taxa de transmissão reduzirá para a próxima taxa mais baixa.
- **b)** Se um nó envia dois quadros a seguir sem receber uma confirmação (uma indicação implícita de erros de bit no canal), a taxa de transmissão volta para a próxima taxa mais baixa. Se forem confirmados 1000 quadros a seguir, ou se um timer que acompanhar o tempo desde o último feedback expirar, a taxa de transmissão aumentará para a próxima taxa mais alta.

- **c)** Se um nó envia dois quadros a seguir sem receber uma confirmação (uma indicação implícita de erros de bit no canal), a taxa de transmissão volta para a próxima taxa mais baixa. Se forem confirmados 10 quadros a seguir, ou se um timer que acompanhar o tempo desde o último feedback expirar, a taxa de transmissão aumentará para a próxima taxa mais alta.
- **d)** Se um nó envia vinte quadros a seguir sem receber uma confirmação (uma indicação implícita de erros de bit no canal), a taxa de transmissão volta para a próxima taxa mais baixa. Se forem confirmados 10 quadros a seguir, ou se um timer que acompanhar o tempo desde o último feedback expirar, a taxa de transmissão aumentará para a próxima taxa mais alta.
- **e)** Se um nó envia dois quadros a seguir recebendo poucas confirmações (uma indicação implícita de erros de bit no canal), a taxa de transmissão volta para a próxima taxa mais baixa. Se forem confirmados 10 quadros a seguir, ou se um timer que acompanhar o tempo desde o último feedback expirar, a taxa de transmissão aumentará para a próxima taxa mais alta.

Técnicas de Segurança em uma WLAN 802.11

Em relação à segurança em redes de computadores sem fio baseadas nas especificações do padrão IEEE 802.11, os protocolos mais conhecidos são o WEP (*Wired Equivalent Privacy*), cujo próprio nome sugere, deve fornecer um nível de segurança semelhante ao encontrado em redes com fio, e o padrão 802.11i, uma versão fundamentalmente mais segura do 802.11, que apresenta algumas importantes falhas de segurança.

O Protocolo WEP (*Wired Equivalent Privacity*)

O protocolo IEEE 802.11 WEP foi desenvolvido em 1999 para fornecer autenticação e criptografia de dados entre um host e um ponto de acesso sem fio (ou seja, estação base) usando uma abordagem de chave compartilhada simétrica. O WEP não especifica um algoritmo de gerenciamento de chaves, portanto, pressupõe-se que o host e o ponto de acesso sem fio tenham concordado de alguma forma com a chave por meio de um método fora da banda.

A autenticação é realizada da seguinte maneira:

1. Um host sem fio solicita autenticação por um ponto de acesso.
2. O ponto de acesso responde à solicitação de autenticação com um **sinal** de valor de 128 bytes.
3. O host sem fio criptografa o **sinal** usando a chave simétrica que ele compartilha com o ponto de acesso.
4. O ponto de acesso descriptografa o **sinal** criptografado pelo host.

Se o **pacote** descriptografado corresponder ao valor do **pacote** originalmente enviado ao host, o host será autenticado pelo ponto de acesso.

Existem várias preocupações adicionais de segurança com o WEP também. Uma conhecida fraqueza do algoritmo explora o algoritmo RC4 quando certos caracteres fracos são escolhidos. Outra preocupação com o WEP envolve os bits CRC transmitidos no quadro 802.11 para detectar bits alterados na carga útil. No entanto, um invasor que altera o conteúdo criptografado e o adiciona em um quadro WEP pode produzir um quadro 802.11 que será aceito pelo receptor.

O Protocolo 802.11i

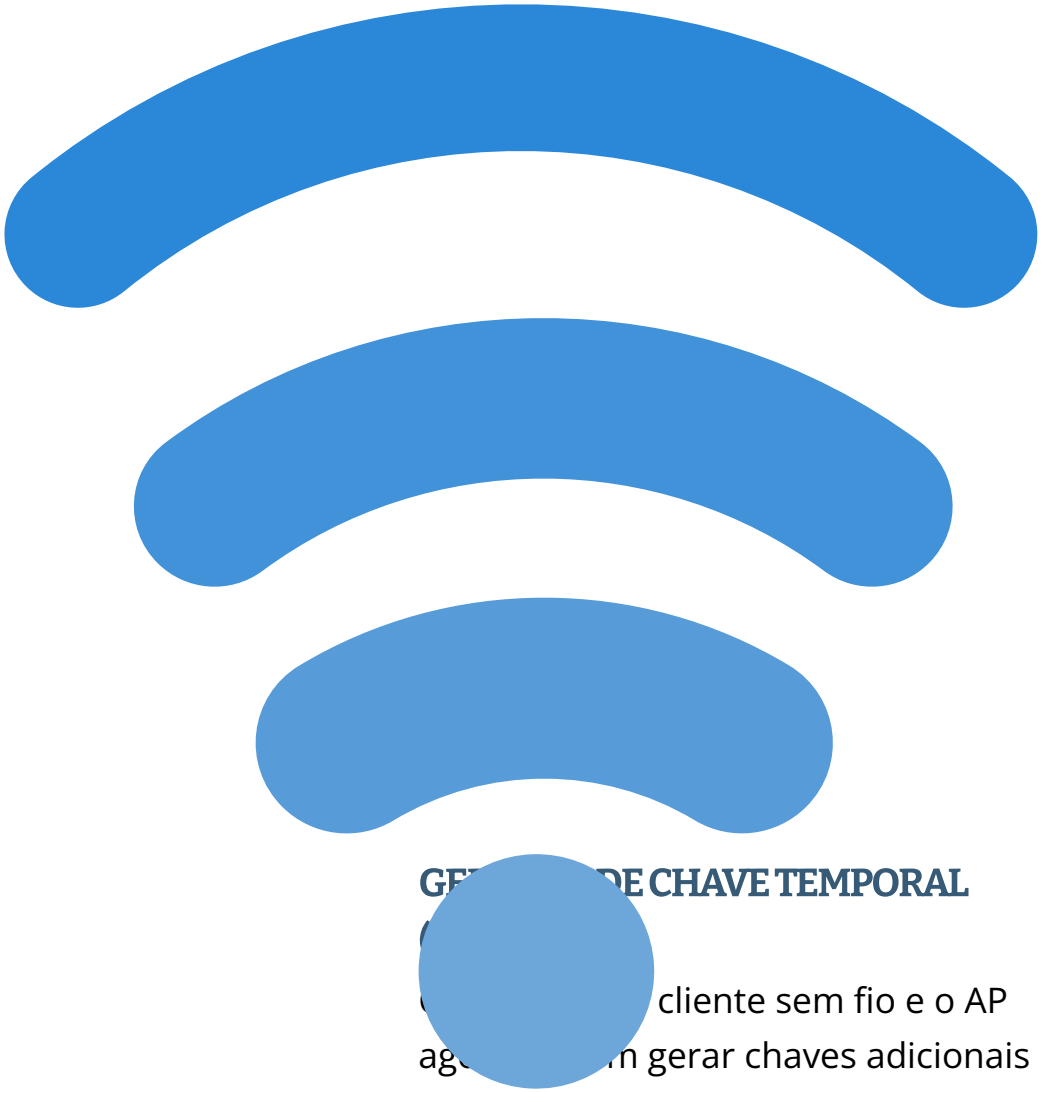
Após o lançamento do IEEE 802.11 em 1999, começaram os trabalhos de desenvolvimento de uma nova versão melhorada do 802.11 com mecanismos de segurança mais fortes. O novo padrão, conhecido como 802.11i, passou pela ratificação final em 2004.

Enquanto o WEP fornece criptografia relativamente fraca, apenas uma maneira de executar autenticação e nenhum mecanismo de distribuição de chaves, o IEEE 802.11i fornece formas muito mais fortes de criptografia, um conjunto extensível de mecanismos de autenticação e um mecanismo de distribuição de chaves.

Além do cliente sem fio e do ponto de acesso, o 802.11i define um servidor de autenticação com o qual o AP pode se comunicar. A separação do servidor de autenticação do ponto de acesso permite que um servidor de autenticação

atenda a vários pontos de acesso, centralizando as decisões (geralmente sensíveis) relacionadas à autenticação e acesso no servidor único e mantendo os custos e a complexidade do ponto de acesso baixos.

O 802.11I OPERA EM QUATRO FASES



O 802.11i fornece ainda várias outras formas de criptografia, incluindo um

esquema de criptografia baseado em AES e uma versão reforçada da criptografia WEP.

O Wi-fi Protected Access

Como resposta aos problemas apresentados pelo protocolo WEP, a Wi-fi Alliance apresentou o Acesso Protegido por Wi-fi (WPA). Esse modelo foi formalmente adotado um ano antes de o protocolo WEP ser aposentado em 2004. Em sua configuração mais comum, o WPA apresenta-se em conjunto com uma chave pré-compartilhada (WPA-PSK). Um dos maiores diferenciais em termos de segurança em relação ao seu antecessor está no tamanho de suas chaves, algoritmos WPA utilizam chaves de 256 bits, bem maiores se comparadas às chaves de 64 e 128 bits utilizadas pelo sistema WEP.

Dentre o conjunto de mudanças que foram implementadas no WPA, cita-se a inclusão das verificações de integridade das mensagens (o que permite determinar se um invasor capturou e modificou uma mensagem em trânsito), além de um protocolo de integridade de chave temporal (TKIP). Esse protocolo emprega um sistema de chaves por pacote, o que o torna essencialmente mais seguro do que o sistema de chaves fixas, utilizados pelo WEP.

Apesar de trazer melhorias significativas em relação ao WEP, o TKIP, seu principal componente, foi projetado de forma que pudesse ser facilmente implementado por atualizações de firmwares nos dispositivos que já possuíssem o WEP. Para isso ser possível, alguns elementos utilizados no WEP foram ‘reciclados’, trazendo assim algumas vulnerabilidades para o WPA.

Assim como o WEP, o WPA demonstrou possuir uma série de vulnerabilidades. Ainda que suas vulnerabilidades não seguissem o mesmo padrão do WEP, foi provado que o recurso suplementar Wi-fi Protected Setup (WPS), projetado para facilitar a vinculação do dispositivo a outros pontos, servia como porta de entrada para invasores.

O Wi-fi Protected Access II

No ano de 2006, o WPA foi substituído pelo WPA2. Tratava-se de uma nova tentativa de aperfeiçoar o algoritmo. Dentre as diversas alterações sofridas pelo protocolo, está a adição do algoritmo AES e a introdução do Modo de Cifra de Contador com Protocolo de Código de Autenticação de mensagem em Cadeia de Blocos (CCMP), que deveria substituir definitivamente o TKIP, o que não aconteceu, o TKIP ainda persiste no WPA2.

Apesar de mais seguro, o WPA2 ainda possui algumas vulnerabilidades importantes, e a principal delas exige que o invasor já tenha acesso à rede Wi-fi segura, uma vez que o tenha, esse invasor pode acessar determinadas chaves e efetuar ataques a outros dispositivos que estejam na rede.

Outra importante questão relacionada ao WPA2 é a permanência daquela que pode ser considerada sua mais importante vulnerabilidade. Assim como ocorre no WPA, o principal vetor de ataque ao WPA2 é o WPS. Ainda que para invadir uma rede protegida sejam necessárias de 2 a 14h utilizando um equipamento moderno, essa questão mostra-se digna de grandes preocupações relacionadas à segurança. Como indicação para aumentar o nível de segurança, sugere-se que o WPA seja desativado e se possível o firmware do dispositivo atualizado para uma versão do WPA que não ofereça o serviço de WPS.

praticar

Vamos Praticar

Com o objetivo de resolver os problemas apresentados pelo WEP, a Wi-fi Allicance apresentou o Wi-fi Protected Access. Em sua configuração mais comum, o WPA apresenta-se em conjunto com uma chave pré-compartilhada (WPA-PSK). Um dos maiores diferenciais em termos de segurança em relação ao seu antecessor está no

tamanho de suas chaves, algoritmos WPA utilizam chaves de 256 bits, bem maiores se comparadas às chaves de 64 e 128 bits utilizadas pelo sistema WEP.

Mesmo com todas as alterações realizadas em relação ao seu antecessor, o WPA continuou apresentando alguns problemas. Dadas as opções abaixo, qual melhor descreve esses problemas?

- **a)** Assim como o WEP, o WPA demonstrou possuir uma série de vulnerabilidades no recurso de propagação dos sinais, nesse sistema os pacotes trafegam totalmente desprotegidos.
- **b)** Assim como o WEP, o WPA demonstrou possuir uma série de vulnerabilidades no recurso de criptografia dos pacotes que são enviados para os destinatários de rede. A criptografia utilizada não é suficientemente segura.
- **c)** Assim como o WEP, o WPA demonstrou possuir uma série de vulnerabilidades, a principal vulnerabilidade está no recurso adicional WPS - Wi-fi Protected Security, que permite reconfigurar os níveis de segurança do sistema.
- **d)** Assim como o WEP, o WPA demonstrou possuir uma série de vulnerabilidades no recurso suplementar Wi-fi Protected Setup (WPS), projetado para facilitar a vinculação do dispositivo a outros pontos, servia como porta de entrada para invasores.
- **e)** Assim como o WEP, o WPA demonstrou possuir uma série de vulnerabilidades, a principal vulnerabilidade está no recurso adicional WPS - Wi-fi Protected Setup, que facilita a vinculação de novos dispositivos desabilitando os algoritmos de criptografia.

Configuração da Segurança em Redes sem Fio

Para que seja possível obter real segurança em redes sem fio, mais do que dispositivos que possuem recursos capazes de elevar seu nível de segurança, é preciso saber como utilizar tais recursos.

Como exemplo pode-se citar chaves criptografadas; ainda que um sistema de criptografia utilize chaves de 256 ou até mesmo 512 bits (o que tornaria a quebra da criptografia praticamente impossível), caso o usuário utilize uma senha 'fraca', as chances de um invasor lograr sucesso tornam-se elevadas, não pelo fato de a criptografia ser ruim, mas sim pelo fato de o usuário ter escolhido uma senha 'óbvia'.

Além de algoritmos de criptografia robustos, os sistemas de redes sem fio contam com outros recursos que podem elevar o nível de segurança em redes locais corporativas e/ou domésticas.

Filtragem de MAC

A filtragem de endereços MAC consiste de um método de segurança que se

baseia no controle de acesso. Os endereços MAC permitem a utilização de 48 bits por cada endereço e, quando utilizados, determinam quais dispositivos podem ou não acessar a rede.

A configuração dos endereços de MAC permite listar o conjunto dos dispositivos permitidos ou não permitidos em uma rede sem fio. Com isso, acessos indesejados à rede podem ser impedidos. Esse modelo de segurança é frequentemente utilizado em redes corporativas com diversos pontos de acesso. Seu principal objetivo é impedir que clientes acessem a rede. Com esse recurso, é possível configurar os pontos de acesso garantindo que os clientes acessem somente o ***gateway*** padrão, mas não os outros dispositivos da rede, isso também aumenta a eficiência do acesso à rede.

Desvantagens da Filtragem de MAC

A utilização de regras de endereçamento MAC apresenta algumas desvantagens, sendo as principais:

- É demorado e tedioso, especialmente se houver muitos dispositivos habilitados para Wi-Fi, pois precisará obter o endereço MAC para cada dispositivo. A lista de dispositivos permitidos deve ser modificada sempre que for preciso habilitar um novo dispositivo.
- Dois endereços MAC devem ser adicionados ao dispositivo, sendo um para o adaptador com fio e o outro o adaptador sem fio.
- Ele não protege contra hackers experientes.
- Isso pode tornar a rede menos segura, porque agora o hacker não precisará mais quebrar uma senha criptografada WPA2 (a não ser que sejam utilizadas as duas opções de segurança).

Ao examinar o pacote usando hackers ***Wireshark*** com um conjunto de ferramentas como o Kali Linux, você pode acessar a rede, pois pode obter o endereço MAC dos dispositivos permitidos e, em seguida, pode alterar o endereço MAC do dispositivo para o endereço MAC permitido e conectar-se como esse dispositivo. Eles podem usar ataques "deauth" ou "deassoc" que desconectam com força um dispositivo de uma rede Wi-Fi ou usam aireplay-ng para enviar pacotes de desassociação aos clientes e, em seguida, conectar-

se no local do dispositivo.

No entanto, os endereços MAC de clientes sem fio não podem realmente ser alterados porque estão codificados no hardware. Mas alguns críticos descobriram que os endereços MAC podem ser falsificados. Tudo o que um invasor precisa fazer é conhecer um dos endereços válidos. Eles não precisam interromper a criptografia para acessar sua rede ou quebrar sua senha criptografada WPA2, ou seja, eles apenas têm que fingir ser um computador confiável.

A filtragem de MAC impedirá que hackers comuns obtenham acesso à rede. A maioria dos usuários de computadores não sabe como enganar seus endereços MAC e muito menos encontrar a lista de endereços aprovados de um roteador. Ao contrário do filtro de domínio, eles não impedem o tráfego de fluir pela rede.

Uma dúvida geral que surge é como os hackers podem obter nosso endereço MAC se não conseguirem se conectar à rede. É uma fraqueza do Wi-Fi que, mesmo que haja uma rede criptografada WPA2, se os endereços MAC desses pacotes não forem criptografados, um hacker um pouco mais experiente poderá acessar a rede e enviar pacotes utilizando algum endereço MAC clonado de algum outro dispositivo que tenha permissão de enviar e receber pacotes nesta rede. Isso significa que qualquer pessoa com o software de detecção de rede instalado e uma placa sem fio ao alcance da sua rede pode facilmente pegar todos os endereços MAC que estão se comunicando com seu roteador e se passar por algum deles.

Alternativas ao Endereçamento de MAC

Uma solução melhor para controlar pessoas de fora que desejam se conectar à sua rede é usar uma rede Wi-Fi convidada. Isso permitirá que eles permitam que outras pessoas se conectem à sua rede, mas não que eles vejam nada na sua rede doméstica. Você pode comprar um roteador barato e conectar-se à sua rede com uma senha e um intervalo de endereços IP separados para fazer isso.

A criptografia WPA2 é suficiente, pois é muito difícil de decifrar. Mas a chave é

ter uma senha forte e longa. Se alguém quebrar sua criptografia WPA2, não precisará se esforçar para enganar a filtragem de MAC. Se um invasor estiver confuso com a filtragem de endereços MAC, não poderá interromper sua criptografia.

praticar

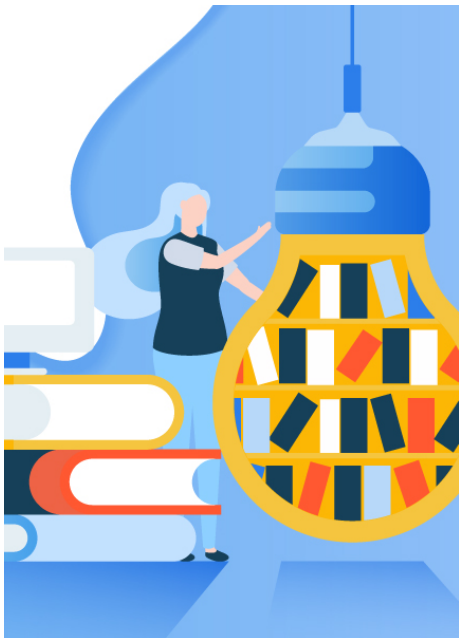
Vamos Praticar

Uma forma de implementar algum tipo de segurança em redes sem fio é através da configuração/criação de listas negras ou brancas contendo os endereços MAC de cada um dos dispositivos que podem ou não acessar a rede. Dessa forma, o dispositivo consegue até mesmo conectar ao ***gateway*** , mas não consegue enviar ou receber pacotes da rede. Sobre a configuração de listas de endereços MAC, qual das opções abaixo está correta?

- **a)** Aplicar o controle de acesso por filtro de endereços MAC tem se mostrado como uma das mais eficazes formas de evitar ataques a redes sem fio.
- **b)** O recurso de controle de acesso por filtro de endereços MAC invalida completamente a utilização de qualquer outro dispositivo de segurança de rede.
- **c)** Apesar de ser um procedimento demorado, a configuração de endereços MAC eleva significativamente a segurança das redes.
- **d)** Trata-se de um procedimento demorado e tedioso, mas que tem diversas vantagens, uma delas é a inibição dos problemas causados pelo WPS.
- **e)** Trata-se de um procedimento demorado e tedioso, principalmente se houver muitos dispositivos para serem adicionados ao access point.

indicações

Material Complementar



LIVRO

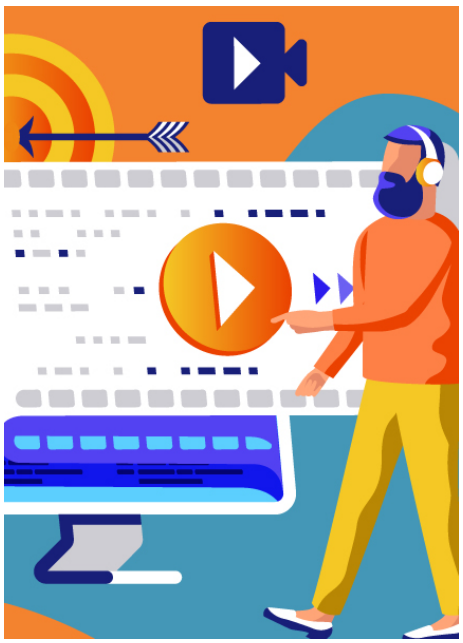
Segurança de Redes sem Fio - Guia do Iniciante

Wrightson, T.; Weber, R. F.

Editora: Bookman, McGraw-Hill Companies, Inc.

ISBN: 978-85-826-0154-9

Comentário: Toda caminhada começa no primeiro passo. Este livro é um ótimo ponto de partida para entender os principais fundamentos relacionados à segurança nas redes sem fio. O conteúdo do livro é didático e intuitivo, além de completo e apropriado para estudantes iniciantes e intermediários.



FILME

O Cibercrime Cotidiano - O que Você Pode Fazer Contra

Ano: 2013

Comentário: Neste talk são discutidas questões relacionadas a crimes digitais, segurança vai muito além de impedir que um hacker invada a sua rede.

TRAILER

conclusão

Conclusão

As redes sem fio não só permitem que dispositivos se conectem a ela sem a necessidade de cabos e fios que podem limitar a mobilidade do dispositivo dentro de uma área, como permitem que os dispositivos migrem de uma rede para outra de forma totalmente transparente, o que é conhecido como mobilidade. Contudo, as redes sem fio apresentam também alguns problemas, sendo a segurança um dos maiores.

É exatamente por ser abrangente, que redes sem fio tendem a ser menos seguras. Entretanto, é possível perceber que existe grande preocupação e esforço na definição e implementação de métodos, algoritmos e políticas de segurança que visam resolver ou ao menos minimizar este problema.

referências

Referências Bibliográficas

CABIANCA, L. A.; BULHMAN, J. H. **Redes LAN / MAN Wireless II** : Funcionamento do Padrão 802.11. 23 maio 2016. Disponível em: http://www.teleco.com.br/tutoriais/tutorialrwlanman2/default.asp . Acesso em: 6 dez. 2019.

ENGST, A.; FLEISHMAN, G. **Kit do Iniciante em Redes Sem Fio** - O Guia Prático sobre Redes Wi-Fi para Windows e Macintosh. 2. ed. [S.l.]: Pearson Makron Books, 2005.

KUROSE, J. F. **Computer networking** : A top-down approach featuring the internet, 3/E. [S.l.]: Pearson Education India, 2005.

RAPPAPORT, T. S. **Comunicação Sem Fio** - Princípios e Práticas. 2. ed. [S.l.]: Pearson Prentice Hall, 2009.

ROCHOL, J. **Sistemas de Comunicação sem Fio** : Conceitos e Aplicações. [S.l.]: Bookman, 2018.

SOARES, L.; MORAES, I. Uma avaliação de vulnerabilidades em protocolos de autenticação para redes sem fio IEEE 802.11. In: ESCOLA REGIONAL DE INFORMÁTICA DO RIO DE JANEIRO (ERI-RJ), 3, 2019, Niterói. **Anais da III Escola Regional de Informática do Rio de Janeiro** . Porto Alegre: Sociedade Brasileira de Computação, apr. 2019 . p. 37-40.

TANENBAUM, A. S.; WETHERALL, D. **Redes de Computadores** . 5. ed. [S.l.]: Pearson, 2011.