Universidade do Minho

Licenciatura em Engenharia Informática

Redes de Computadores

TP3 : Redes Sem Fios (802.11)

1. Objectivos

Este trabalho, previsto para duas aulas, tem como objectivo explorar vários aspectos do protocolo IEEE 802.11, tais como o formato das tramas, o endereçamento dos componentes envolvidos na comunicação sem fios, os tipos de tramas mais comuns, bem como a operação do protocolo.

2. Estudo Prévio

Antes de iniciar o trabalho, é recomendada a leitura dos *slides* sobre Redes sem Fios que foram colocados na plataforma de ensino. Como neste trabalho se aprofundam aspectos da descrição feita nos *slides*, pode consultar outros documentos relacionados, tais como:

- "A Technical Tutorial on the 802.11Protocol," por Pablo Brenner (Breezecom Communications), http://www.sss-mag.com/pdf/802_11tut.pdf e

- "ANSI/IEEE Std 802.11, 1999 Edition (R2003)," http://gaia.cs.umass.edu/wireshark-labs/802.11-1999.pdf.

2.1. Tipos de tramas

Nesta secção é feito um pequeno resumo dos tipos (e subtipos) de tramas 802.11 mais comuns. A Tabela 1 da norma IEEE 802.11 (em anexo) complementa a descrição, sendo útil durante a observação e análise de tráfego WiFi.

Tramas de Gestão (*Management frames*)

As tramas de gestão 802.11 permitem que as estações estabeleçam e mantenham a comunicação. Os subtipos de tramas 802.11 para gestão da ligação de dados são:

- Trama de Autenticação (*Authentication*): a autenticação 802.11 é um processo pelo qual o ponto de acesso (AP) aceita ou rejeita a identidade de um acesso rádio proveniente de uma placa de rede (NIC) 802.11.

- Trama de Termino de Autenticação (*Deauthentication*): Uma estação envia uma trama de termino de autenticação (*deauthentication*) para outra estação ou para o AP se quiser terminar a comunicação de forma segura.

- Trama Pedido de Associação (*Association Request*): A associação 802.11 permite que o AP possa alocar recursos para a ligação e efectuar a sincronização com a interface de rede que efectua o pedido. A NIC da estação inicia o processo de associação através do envio de um pedido de associação ao AP, em que a trama enviada fornece informações sobre a NIC (por exemplo, taxas de dados suportadas) e o identificador público da rede (SSID - *Service Set Identifier*) à qual se pretende associar. Depois de receber o pedido de associação, o AP considera associar-se à interface de rede respectiva, reservando recursos (e.g. espaço de memória) e definindo um ID para a associação.

- Trama Resposta de Associação (*Association Response*): Um AP envia uma trama resposta de associação contendo uma notificação de aceitação ou rejeição face ao pedido de associação formulado. Se o AP aceita a interface rádio, a trama resposta inclui informações sobre a associação, tais como o ID da associação e as taxas de dados suportadas. Sendo a associação estabelecida, a interface da estação pode utilizar o AP para comunicar com as outras estações na rede sem fios, bem como com estações no sistema de distribuição (DS) acessíveis a partir do AP (e.g. rede Ethernet).

- Trama Pedido de Re-associação (*Reassociation Request*): É equivalente ao Pedido de Associação mas aplicável a associações já existentes. Aplica-se, por exemplo, quando uma estação decide associar-se a um novo AP em detrimento do actual, e.g. por receber um sinal melhor.

- Trama Resposta de Re-associação (*Reassociation Response*): É equivalente à Resposta de Associação, mas surge como resposta a um Pedido de Re-associação.

- Trama de Dissociação (*Disassociation*): Uma estação envia uma trama de dissociação para outra estação ou para o AP quando quer terminar a associação. Os recursos alocados à associação podem ser libertados, removendo a interface de rede da tabela de associações.

- Trama de Anúncio (*Beacon*): O AP envia periodicamente tramas *Beacon* para anunciar a sua presença e transmitir informações tais como a data e hora, o SSID, e outros parâmetros relativos ao AP a todas as interfaces rádio que estão dentro do seu alcance rádio. É pela recepção de tramas *Beacon* (*passive scanning*) ou pelo varrimento dos vários canais rádio (*active scanning*) que uma estação pode optar por um AP mais favorável.

- Trama Pedido de Prova (*Probe Request*): A estação envia uma trama *Probe Request* quando precisa obter informações de uma outra estação. Esta trama é útil, por exemplo, para uma placa de rede tentar determinar quais os pontos de acesso que estão dentro do seu alcance rádio (*active scanning*).

- Trama Resposta de Prova (*Probe Response*): A estação ou AP irão responder com uma trama de *Probe Response*, contendo informações sobre as taxas de dados suportadas, etc.

Tramas de Controlo (*Control Frames*)

Este tipo de tramas permitem auxiliar a troca de tramas de dados entre as estações sem fios. Como subtipos comuns de tramas de controlo 802.11 tem-se:

- Trama Pedido para Enviar (*RTS - Request to Send*): Na norma 802.11, a função RTS/CTS é opcional e tem como objectivo reduzir colisões causadas, por exemplo, por estações escondidas, i.e. estações que têm associações com o mesmo AP mas não se vêem entre si. Assim, numa fase preliminar, uma estação pode enviar uma trama RTS para outra estação, aguardando uma trama de resposta CTS antes de enviar a trama de dados. Sendo as tramas RTS/CTS de pequeno tamanho a probabilidade de colisão é reduzida.

- Trama Resposta com indicação para enviar (*CTS - Clear to Send*): Uma estação responde a um RTS com uma trama CTS, dando indicação à estação para enviar dados. O CTS inclui um valor de temporal que faz com que todas as outras estações (incluindo estações ocultas) adiem a transmissão de tramas por um período necessário para que o envio de dados previamente solicitado se processe sem colisões.

- Trama Confirmação da recepção (*ACK - Acknowlegment*): Depois de receber uma trama de dados, a estação de recepção irá utilizar um código de verificação para detectar a presença de erros. A estação receptora envia uma trama ACK para a estação emissora, se não forem encontrados erros. Se a estação emissora não receber um ACK depois de um certo período de tempo, a estação emissora retransmite a trama.

Tramas de Dados (*Data Frames*)

O principal objetivo de uma LAN sem fios é obviamente proporcionar a transmissão e comunicação de dados. Como tal, a norma IEEE 802.11 define um tipo específico de trama de dados que podem ser facilmente identificados com um analisador de tráfego (e.g. wireshark). As tramas do tipo DATA têm vários subtipos para usos específicos.

2.2. Limitações na captura de tráfego WiFi

Como explicado na documentação de apoio do Wireshark[1], a maioria dos *device drivers* para as placas de rede *wireless* 802.11 (particularmente para o sistema operativo Windows) não disponibilizam a opção de capturar e copiar as tramas 802.11 para análise no Wireshark. Em contrapartida, as placas de rede 802.11 transformam normalmente as tramas de dados 802.11 em falsas tramas Ethernet antes de as disponibilizar ao *host*. Isto é, os detalhes de cada trama 802.11 e o funcionamento da rede sem fios são ocultados/ignorados antes de passar a trama à pilha protocolar do sistema operativo e ao mecanismo de captura de pacotes. Por esta razão, a captura de tramas nas interfaces Ethernet ou WiFi não evidencia qualquer diferença quando analisadas no Wireshark.

Como o sucesso na captura de tráfego WiFi depende de factores tais como, as versões do Wireshark e do sistema operativo em uso, e dos *device drivers* de cada placa, sugere-se que na realização do trabalho os alunos usem preferencialmente capturas previamente realizadas e disponibilizadas na plataforma de apoio ao ensino.

A título unicamente experimental os alunos podem também realizar capturas de tráfego 802.11, usando uma de duas abordagens:
(a) via GUI, selecionar *Edit/Preferences/Capture* e para a interface WiFi (e.g. en1) escolher as opções *Monitor Mode*, com o *Default link-layer header type* do tipo 802.11.
(b) via CLI, invocar `wireshark -i en1 -I -y IEEE801_11&`.

3. Primeiros Passos

Descarregue da plataforma de ensino a captura *Wireshark_802_11.pcap* [J.Kurose, K.Ross] e abra o ficheiro no Wireshark. Este *trace* foi capturado usando o *AirPcap* e o *WireShark* no computador de um dos autores, numa rede com um *Access Point /Router* Linksys 802.11, com dois PCs ligados por cabo ao AP e um *laptop* ligado sem fios. Existe também acesso a outros APs vizinhos.

Na captura realizada, destacam-se as seguintes atividades associadas ao *laptop* ligado à rede WiFi. No início da captura, este está já associado ao AP designado 30 Munroe St.

- aos t=24.82s o *host* faz um pedido HTTP a http://gaia.cs.umass.edu/wireshark-labs/alice.txt. O endereço IP do gaia.cs.umass.edu é 128.119.245.12.

[1] http://wiki.wireshark.org/CaptureSetup/WLAN

- aos t=32.82s, o *host* faz um pedido HTTP ao http://www.cs.umass.edu cujo endereço IP é o 128.119.240.19.
- aos t=49.58s o *host* desconecta-se do AP 30 Munroe St e tenta ligar-se ao AP linksys_ses_24086. Trata-se de um AP sem acesso aberto pelo que o host eventualmente não consegue ligar-se a este AP.
- aos t= 63.0s, o *host* desiste de tentar associar-se ao linksys_ses_24086 e associa-se de novo ao AP 30 Munroe St.

Uma vez que o *host* e o AP referidos não são os únicos dispositivos que usam o Canal 6, haverão muitas outras tramas na captura. Um exemplo são as tramas de *beacon* anunciadas por um AP vizinho a operar também no Canal 6.

4. Acesso Rádio

Como pode ser observado, a sequência de bytes capturada inclui informação do nível físico (rádio), para além dos *bytes* correspondentes a tramas 802.11.

1) Selecione uma trama da ligação e identifique em que frequência do espectro está a operar a rede sem fios e a que débito foi enviada a trama escolhida.
2) Qual o número e o tipo do canal que está a ser usado para a comunicação rádio?
3) Indique qual o índice de qualidade do sinal.

5. Tramas Beacon

Recorda-se que as tramas *beacon* são usadas pelos APs 802.11 para anunciar a sua existência. Para o trace em uso:

4) Qual o tipo de uma trama *beacon*? Indique quais os seus identificadores de tipo e subtipo. Em que parte da trama estão especificados?
5) Identifique os SSIDs dos APs (*Access Points*) que estão a operar na rede e diga qual tende a proporcionar a melhor qualidade de sinal?
6) Para dois dos APs identificados, indique quais são os intervalos de tempo previstos entre as transmissões de tramas *beacon*? (nota: este valor é anunciado na própria trama *beacon*).
7) Na prática, a periodicidade de tramas *beacon* é verificada? Tente explicar porquê?
8) Identifique e registe todos os endereços MAC usados nas tramas *beacon* enviadas pelos APs? Recorde que fonte, destino e BSS ID são endereços contidos no cabeçalho das tramas 802.11. Para uma descrição detalhada da estrutura da trama 802.11, veja a secção 7 da norma IEEE 802.11 (citada acima).
9) As tramas *beacon* anunciam que o AP pode suportar vários débitos de dados base assim como vários "*extended supported rates*" adicionais. Quais são esses débitos?

6. Transferência de Dados

Uma vez que a colecta de tráfego começa com o *host* já associado com o AP, vamos concentrar primeiro a atenção para a transferência de dados sobre uma associação 802.11, antes de analisar o processo de associação/desassociação.

Recorda-se que neste trace, aos t=28.42s, o *host* faz um pedido HTTP para http://gaia.cs.umass.edu/wireshark-labs/alice.txt. 128.119.245.12 é o endereço IP do gaia.cs.umass.edu. Então, aos t=32.82, o *host* faz um pedido HTTP ao http://www.cs.umass.edu.
Um pedido HTTP, correndo sobre um protocolo de transporte orientado à conexão como

o TCP (*Transmission Control Protocol*), é antecedido pelo estabelecimento de uma conexão TCP.

10) Localize a trama 802.11 que contenha o segmento TCP SYN para a primeira conexão TCP (que descarrega alice.txt). Quais são os três campos de endereço contidos na trama 802.11? Qual o endereço MAC correspondente ao *host* ligado sem fios? E ao AP? E ao router de acesso (primeiro salto)? Qual é o endereço IP do *host* sem fios que envia este segmento TCP? Qual é endereço IP de destino? A que sistema corresponde esse endereço IP destino?
11) Localize a trama 802.11 que contém o segmento TCP SYN ACK para esta conexão TCP. Quais são os três campos de endereços MAC contidos na trama 802.11? Que endereço MAC corresponde ao *host*? O endereço MAC do originador da trama corresponde ao endereço IP do dispositivo que envia o segmento TCP encapsulado no datagrama? (nota: este aspecto deve ter ficado claro com a realização do TP2).
12) Que tipo de tramas de controlo 802.11 ocorrem na transferência de dados realizada? Quando ocorrem?

7. Associação e Desassociação

Recorde-se que um *host* deve associar-se a um ponto de acesso antes de enviar dados. A associação nas redes sem fios 802.11 é executada usando a trama ASSOCIATION REQUEST (enviada do host para o AP, com a trama de tipo 0 e sub-tipo 0) e a trama ASSOCIATION RESPONSE (enviada pelo AP para o *host*, em resposta ao ASSOCIATION REQUEST recebido). Para uma explicação mais detalhada pode consultar a Secção 5.7, pág.25 e a Secção 7.2.3, pág.45, da especificação 802.11 (ver documento 802.11-1999.pdf).

13) Que ação é tomada pelo *host* após t=49.5s que determina a quebra de associação com o AP 30 Munroe St que existia desde que a captura de tramas começou? Como interpreta as tramas 802.11 subsequentes relacionadas com a anterior ação? Segundo a especificação IEEE 802.11, há alguma trama que seria esperada, mas não aparece?

14) Examine o ficheiro de *trace* e procure tramas de autenticação enviadas pelo *host* para o AP e vice-versa (se filtrar os resultados por `wlan.fc.type_subtype` ajuda a localização). Quantas tramas de AUTHENTICATION são enviadas do *host* sem fios para o AP linksys_SES_24086 AP? Durante que período de tempo?

15) O *host* tenta usar algum algoritmo de autenticação/chave ou tenta aceder de forma aberta? Existe alguma resposta do AP linksys_SES_24086 ao pedido de autenticação? Porquê?

16) Identifique as ações 802.11 (após t=63.16s) que decorrem do comportamento analisado na questão anterior e quais os sistemas envolvidos? Usando um filtro apropriado, registe a janela do wireshark que ilustre as tramas de gestão trocadas que ajuda a fundamentar a sua resposta.

17) Caracterize a nova associação do *host* com o AP (30 Munroe St).

8. Probing

O trace disponibilizado contém tramas PROBE REQUEST e PROBE RESPONSE, comuns na operação das redes WiFi. Estabeleça um filtro adequado para localizar simultaneamente estes subtipos de trama de uma forma rápida e eficiente.

18) Quais são os endereços MAC do originador, receptor e BSS ID nestas tramas? Qual é a função deste tipo de tramas?

9. Opções RTS/CTS

A amostra de tráfego 802.11b usada anteriormente não usa a opção RTS/CTS na troca de dados entre as estações e o AP. Com o intuito de estudar esta variante do controlo de acesso ao meio, considere o trace *crc2013-eduroam.pcap* recolhido numa rede 802.11g também disponibilizado na plataforma de ensino.

19) Certifique-se do tipo de canal que está a ser usado e identifique todos os APs que estão a ser anunciados.
20) Tomando como exemplo a estação cujo endereço MAC é `HonHaiPr_27:46:a2 (0c:60:76:27:46:a2)`, identifique a ocorrência de troca de dados envolvendo tramas de controlo RTS/CTS. Verifique a seu sentido de envio (toDS, fromDS). Registe o endereçamento MAC dos sistemas envolvidos, explicando o seu papel no processo de troca de dados.

10. Relatório do trabalho realizado

O relatório do TP3 deve incluir:

- uma secção "Questões e Respostas" relativas ao enunciado acima;

- uma secção de "Conclusões" que autoavalie e resuma os resultados da aprendizagem nas várias vertentes estudadas no trabalho.

O relatório deve seguir o formato habitual (LNCS) e ser submetido na plataforma de ensino com o nome RC-TP3-PL<TurnoGrupo>.pdf (por exemplo, RC-TP3-PL11.pdf para o grupo PL1.1) no final da aula prevista para conclusão do trabalho.

Créditos: Parte deste trabalho é baseado no Wireshark Lab 802.11 [J. Kurose e K. Ross].

Anexo

Table 1—Valid type and subtype combinations

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110–0111	Reserved
00	Management	1000	Beacon
00	Management	1001	Announcement traffic indication message (ATIM)
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101–1111	Reserved
01	Control	0000–1001	Reserved
01	Control	1010	Power Save (PS)-Poll
01	Control	1011	Request To Send (RTS)
01	Control	1100	Clear To Send (CTS)
01	Control	1101	Acknowledgment (ACK)
01	Control	1110	Contention-Free (CF)-End
01	Control	1111	CF-End + CF-Ack
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000–1111	Reserved
11	Reserved	0000–1111	Reserved