|  |  |  |  |
| --- | --- | --- | --- |
| **《计算机网络》实验报告** | | | |
| **实验编号** | 实验3 | **实验名称** | 802.11 |
| **姓名** | 杨伟康 | **学号** | 202200201095 |
| **班级** | 网安班 | **成绩** | （空着） |
| 1. **实验目的**   探索802.11的物理层、链路层和管理功能。它被广泛用于将移动设备无线连接到互联网，并且在你课本的§4.4节中有所涵盖。首先回顾那一节。 | | | |
| 1. **实验要求**   Wireshark：这个实验使用了Wireshark软件工具来捕获和检查数据包跟踪。数据包跟踪是网络上某个位置处流量的记录，就像对穿过特定线路的所有比特位进行快照一样。数据包跟踪为每个数据包记录时间戳，以及组成数据包的位，包括从低层头部到高层内容。 | | | |
| 1. **实验内容** 2. Fetch a Trace 3. Inspect the Trace 4. 802.11 Physical Layer 5. 802.11 Link Layer 6. 802.11 Management | | | |
| 1. **实验过程**   Step 1: Fetch a Trace  启动跟踪文件trace-80211.pcap，您可以找到跟踪文件并直接打开它以使用跟踪文件启动Wireshark。启动结果如下：    Step 2: Inspect the Trace  首先，我们将查看802.11帧的格式。在跟踪记录中，会捕获到许多不同类型的802.11帧；Info字段描述了帧的类型，如Beacon、Data和Acknowledgement。我们将检查一个Data帧，它用于在802.11网络上传输数据包。  在跟踪记录中找到一个Data帧并选择它。Wireshark允许我们选择一个帧（从顶部面板）并查看其协议层，包括头部字段（在中间面板）和组成帧的字节（在底部面板）。在下面的图中，我们已经选择了一个Data帧:    **检查与该帧一起记录的这些协议的协议层。查看中间面板。**  Frame 是 Wireshark 添加的一个记录，包含了帧的时间和长度信息；它并没有捕获“空中”传输的比特。  Radiotap 也是 Wireshark 创建的一个记录，用于捕获物理层参数，如信号的强度和调制方式。现在先跳过这个记录；我们稍后会研究它。  IEEE 802.11 是 802.11 Data 帧的比特。这是我们正在寻找的记录，稍后会详细探讨它。在图中，它被选中并展开，以便您可以看到其内部字段（在中间面板）以及它所占用的帧的部分（在底部面板中高亮显示，并在底部标识为 28 字节长）。  Data 是一个包含帧有效载荷数据的记录，即包含更高层协议的数据，如 LLC、IP 数据包等。或者，您可能直接看到这些更高层协议本身.    **展开 Data 帧的 IEEE 802.11 记录，并检查各个头部字段的详细信息。**您可以使用“+”扩展器或图标来展开这个区块；在我们的图中，它已经被展开。要检查这些字段，您可以将其与图 4-29 进行比较。Wireshark 中的字段包括：  • Frame Control（帧控制）：它编码了帧的类型和子类型（例如 Data），以及各种标志。我们稍后会详细查看这些字段。  • Duration（持续时间）：该字段告诉计算机在无线介质上完成此次交换所需的额外数据包所需的时间。  • BSS 标识符、源地址和目标地址，顺序取决于 Data 帧的具体内容。这些地址字段用于标识发送数据包的设备以及应该接收数据包的设备。BSS 标识符是无线接入点的地址。  • Fragment（片段）和 Sequence Number（序列号）：这些字段用于在需要时重新组装和重传帧。每次新的传输时，序列号都会递增。  • Frame Check Sequence（帧校验序列）：这是帧上的 CRC（循环冗余校验）。它位于帧的末尾（点击它您将看到它在帧中的位置），但为了方便起见，它被列在其他 802.11 头部字段中。  • 如果帧有效载荷被加密，那么可能还有一个 WEP 或 WPA2 字段包含安全参数。我们在这里不深入探讨无线安全，因此您可以忽略该字段。    **最后，展开 Frame Control 字段并详细查看它，包括其中的 Flags。**  所有 802.11 帧都以一个 Frame Control 字段开始，其子字段和标志的详细信息决定了消息的其余部分的格式；它可能类似于我们上面探索的 Data 帧，或者完全不同，比如我们稍后会查看的 Ack 帧。子字段包括：  • Version（版本）：当前版本的值为 0。  • Type（类型）和 Subtype（子类型）：指定帧的类型，例如 Data 或 Ack。  • To DS（到达 DS）：如果帧是通过 AP 从计算机发送到有线网络，则设置此标志。  • From DS（来自 DS）：如果帧是通过 AP 从有线网络发送到计算机，则设置此标志。  • More fragments（更多片段）：如果此消息中还有更多帧，则设置此标志。  • Retry（重试）：如果帧是重传，则设置此标志。  • Power management（电源管理）：如果发送方在传输后将进入省电睡眠模式，则设置此标志。  • More data（更多数据）：如果发送方有更多帧要发送，则设置此标志。  • Protected（已保护）：如果帧使用 WEP/WPA2 加密，则设置此标志。  • Order（顺序）：如果接收方必须按顺序保持帧的顺序，则设置此标志。  这些标志和子字段为网络中的设备提供了关于如何处理帧的重要信息。通过查看这些字段，您可以更深入地了解帧的用途和它在网络中的位置。  Step 3: 802.11 Physical Layer  首先从物理层开始。在最低层，发送和接收消息主要涉及频段、调制和信号接收的信噪比。我们可以使用Radiotap头中的信息来查看所有这些因素！  频道频率是什么？ 要找到频率，请展开任何帧的Radiotap头，并查找“Channel frequency”字段。这个字段将显示该帧使用的频道频率。在大多数情况下，跟踪中的所有帧的频道频率都是相同的，因为无线网络接口被设置为监听一个固定的频率。  要查看调制方式，我们可以观察“Data Rate”值，而要查看信噪比（SNR），我们可以观察“SSI Signal”值（结合“SSI Noise”值）。“SSI Signal”值更常见地被称为RSSI（Received Signal Strength Indication，接收信号强度指示）。这些字段在不同的帧中会有所不同。    通过转到“Preferences”面板（在“Edit”菜单下），然后选择“Columns”（通过展开“User Interface”块），为TX Rate（或Data Rate）和RSSI（或SSI Signal值）添加两个新的显示列。在我们的图中，这两列分别被命名为“Rate”，其字段类型为“IEEE 802.11 TX Rate”，以及“RSSI”，其字段类型为“IEEE 802.11 RSSI”。你可以重新排列这些列，以便这些列位于“Info”列的左侧，以便更好地查看。当你返回到主显示界面时，你将看到每个帧的Rate和RSSI信息。    更改后结果如下    **使用的是哪些速率？请按照从低到高的顺序列出这些速率。**    **在跟踪中，RSSI的范围是多少，因此SNR的变化范围是多少？请给出最强和最弱的RSSI以及它们之间的dB差值。**  RSSI的范围是-69dBm到-44dBm，差值是25dBm  SNR的变化范围是21dBm到47dBm  Step 4: 802.11 Link Layer  在统计菜单栏的会话中选择802.11。这将打开一个窗口，类似于下面的图例，其中列出了每一对正在通信的计算机。你可以通过点击“Packets”或“Bytes”列标题来按大小对此列表进行排序。  **最活跃的无线通信会话使用的BSS ID是什么？**  BSS ID值用于标识接入点（AP），所以这个BSS ID标识了最活跃的AP，很可能是我们正在监控的AP。为了找到它，你可以通过点击列标题来对源或目的地址进行排序。  为了查看不同类型的流量数量，我们可以检查802.11帧。802.11帧可以是数据帧、控制帧或管理帧。这些帧通过帧控制字段中的Type子字段的值来区分。你可以检查不同的数据包以查看不同类型帧的值。  要过滤仅查看数据帧，请在顶部面板中的帧列表上方的“Filter”框中输入表达式“wlan.fc.type==2”。点击Type子字段时，底部的状态显示会告诉我们Wireshark通过名称wlan.fc.type知道这个字段。因此，用于过滤Type值为2的数据帧的表达式是“wlan.fc.type==2”。  当你在Filter框中输入此表达式后，显示应类似于下面的图例。应用此过滤器后，底部的状态行将告诉你显示了多少个跟踪数据包。这告诉你跟踪中有多少数据帧。根据Subtype子字段的值，可能有几种不同的数据帧，如Info列所示。你可以点击此列标题以按帧类型排序，以查看哪些类型是最普遍的。    **在跟踪数据中，有多少数据帧？最常见的数据帧子类型是什么？**  有1783个数据帧，最常见的为  3540 42.385412 CiscoLinksys\_e3:e9:8d Apple\_ac:6c:26 802.11 129 36.0 -58 dBm Data, SN=3526, FN=0, Flags=.p....F.C  跟踪中有多少控制帧，最常见的子类型是什么？  有1391个控制帧，最常见的为  3539 42.376468 Apple\_ac:6c:26 (10:9a:dd:ac:6c:26) (RA) 802.11 39 24.0 -58 dBm Acknowledgement, Flags=........C  结果如图：    跟踪中有多少管理帧，最常见的子类型是什么？  有531个管理帧，最常见的是  3529 42.291503 CiscoLinksys\_e3:e9:8f Broadcast 802.11 109 1.0 -57 dBm Beacon frame, SN=3524, FN=0, Flags=........C, BI=100, SSID="djw"    **列出在确认帧（Acknowledgement frame）中按顺序发送的IEEE 802.11字段以及它们的字节长度。不要将帧控制字段（Frame Control field）拆分为子字段，因为我们已经查看了这些细节。**  以下是IEEE 802.11确认帧中按顺序发送的字段以及它们各自的长度（以字节为单位）：   1. **Frame Control**（帧控制）：这是一个固定长度的字段，通常为2字节。它包含了帧的类型、子类型以及其他控制信息。 2. **Duration/ID**（持续时间/ID）：这个字段的长度根据帧的类型和配置而有所不同，但在确认帧中，它通常用于表示剩余的发送时间（以便其他设备可以等待这段时间后再发送数据以避免冲突）。在确认帧中，这个字段可能是2字节。 3. **Address 1**（地址1）：这个字段是接收方的MAC地址，长度为6字节。 4. **FCS**（帧校验序列）：这是一个用于检测帧在传输过程中是否出现错误的字段，通常为4字节。   所以，一个IEEE 802.11确认帧的大致字段顺序和长度（以字节为单位）为：   * Frame Control: 2字节 * Duration/ID: 2字节（具体长度可能根据网络配置有所不同） * Address 1: 6字节 * FCS: 4字节   使用过滤器表达式来查找原始数据帧和重传数据帧的数量。例如，“wlan.fc.type==2 && wlan.fc.retry==0”将找到原始数据帧。    **估算重传率作为重传次数与原始传输次数的比率。展示你的计算过程。**  根据上面的过滤的结果有1430个原始传输，重传次数为3731-1430=2301个  重传率为2301/1430=161％  **发送到AP的帧中有多少比例的帧表示客户端正在关闭电源？**    比例为16/3731  Step 5: 802.11 Management  展开信标帧的有效载荷以查看其参数，并回答以下问题：  **主AP的SSID是什么？这是信标帧中的一个标记参数。**    **主AP的信标帧多久发送一次？你可能在信标帧本身中找到信标间隔，或者将时间显示更改为显示自上一帧以来的间隔。（在“视图”下，选择“时间显示格式”，然后选择“自上一显示数据包起的秒数”。）**    **主AP支持哪些数据速率？这些速率在标记参数下列出。**    **信标帧传输的速率是多少？这个问题的答案可以在Radiotap头部找到，或者更方便地在你之前步骤中添加的列中显示**。    **关联请求/关联响应帧的Type和Subtype值是什么？**  关联请求（Association Request）和关联响应（Association Response）帧在IEEE 802.11无线局域网标准中属于管理帧（Management Frames）的范畴。  对于关联请求帧：  Type: Management（管理帧）  Subtype: Association Request（关联请求）  在Wireshark中，你可能会看到Subtype的十六进制值，这取决于具体的实现和版本，但通常关联请求的Subtype会是一个特定的值，标识为关联请求。  对于关联响应帧：  Type: Management（管理帧）  Subtype: Association Response（关联响应）  **探测请求/探测响应帧的Type和Subtype值是什么？**  探测请求（Probe Request）和探测响应（Probe Response）帧在IEEE 802.11无线局域网标准中属于管理帧（Management Frames）的一部分。这些帧用于客户端设备在尝试连接到无线网络时搜索可用的接入点（AP）。  对于探测请求帧（Probe Request）：  Type: Management（管理帧）  Subtype: Probe Request（探测请求）  在Wireshark中，你可能会看到Subtype的十六进制值，但通常探测请求的Subtype会被明确标识为Probe Request。  对于探测响应帧（Probe Response）：  Type: Management（管理帧）  Subtype: Probe Response（探测响应）  Explore on your own  **完成这个实验室后，我们鼓励你自行深入探索802.11协议。我们已经涵盖了多个主题的基础知识，每个主题你都可以进一步深入研究。以下是一些建议的方向：**  **• 观察一个给定的客户端如何随时间使用不同的速率。这被称为速率适应。**  **• 查看哪些客户端正在使用电源管理，并尝试理解它们的休眠行为。**  **• 看看你是否能找到使用RTS/CTS机制的客户端。**  **• 查找探测请求序列，观察计算机何时发送它们，以及你可以从中了解到什么。**  **• 使用WEP/WPA2密钥配置Wireshark，以查看从LLC层开始的802.11有效载荷。**  **• 尝试用从你自己的网络中获取的跟踪文件来执行上述所有操作。** | | | |
| **四．实验心得**  深刻理解了802.11协议的多层次结构：802.11不仅是一个简单的无线连接协议，它包含了物理层、链路层和管理层等多个层次，每个层次都有其特定的功能和职责。通过实践，我更加深入地理解了这些层次是如何协同工作以确保无线网络的稳定性和效率。  对无线网络的安全性有了更深刻的认识：通过配置和分析WEP/WPA2密钥，我意识到无线网络的安全性至关重要。了解如何保护无线网络的传输数据，以及如何在网络攻击中保持安全性，是我在这次实验中获得的宝贵知识。 | | | |