WLAN标准中三种加密模式的安全性比较

袁昊男 2018091618008

【摘要】无线局域网（WirelessLAN，简称WLAN）是近年来发展迅速的无线数据通信网。安全性能成为无限局域网的关键性能之一。本文对比分析了目前无线局域网主要使用的三种加密模式：WEP模式、TKIP模式和CCMP模式，对其进行安全性分析。

【关键词】无线安全；WLAN；WEP；TKIP；CCMP

1 概述

1997年，IEEE组织推出的无线局域网（WLAN）标准802.11，是在无线局域网领域内的第一个被国际上认可的无线标准。由于该标准在速率和传输距离上都不能满足人们的需要，1999年IEEE小组又相继推出了802.11b“High Rate”和802.11a两个新标准，而后又推出了802.11g标准。IEEE802.11委员会推出最新的802.111标准，以提升移动用户的无线局域网的安全性能。随着WLAN标准的推出，802.11的安全问题成为无线网络的焦点。在传统的有线网络上，一个攻击者可以物理接入到有线网络内或设法突破边缘防火墙或路由器。对一个无线网络而言，所有潜在的无线攻击者只需要携带其可移动设备呆在一个舒服的位置，用无线嗅探程序就可展开工作。

2 WEP加密模型及其安全性分析

**2.1 WEP加密模型**

WEP是Wired Equivalent Privacy的简称，该协议模型是由802.11标准定义的安全性协议模型，用于在无线局域网中保护链路层数据。WEP安全协议中使用40位密钥（KEY），采用的是由RSA组织开发的RC4对称加密算法，RC4是密钥长度可变的流加密算法簇，在链路层对传输的数据进行加密。

WEP的封包格式（数据包格式）如图2-1-1所示。



图2-1-1 WEP数据包格式

WEP数据包由初始化向量IV（Initialization Vector）、数据Data、完整性校验值ICV（Integrity Check Value）三个部分构成。

WEP协议支持64位和128位的密钥加密。对于64位加密，加密密钥为10个十六进制字符（0-9和A-F）或5个ASCII字符，相对应的就是40位密钥加上这24位初始化向量所组成的，也称为WEP-40；对于WEP协议128位加密，加密密钥为26个十六进制字符或13个ASCII字符，也会被称为104位加密，相应的128位的前104位是加密密钥，后24位是初始向量。

WEP协议主要依赖通信双方共享的密钥来保护所传的加密数据帧。WEP也提供认证功能，当加密机制功能启用，STA要尝试连接上AP时，AP会发出一个Challnge Packet，STA再利用共享密钥将此值加密后送回接入点以进行认证比对，只有认证结果正确无误，才能获准使用接入点网络的资源。WEP-40具有很好的互操作性，所有通过Wi-Fi组织认证的产品都可以实现WEP互操作。

WEP加密方法使用共享密钥和RC4加密算法。接入点AP和连接到该接入点的所有STA必须使用同样的共享密钥。对于通信过程中任一方向发送的数据包，传输过程都将数据包的内容与数据包的检查和组合在一起。然后，WEP标准要求传输过程中创建一个特定于数据包的初始化向量IV，与密钥相组合在一起，用于对数据包进行加密。接收器生成自己的匹配数据包密钥并用之对数据包进行解密。在理论上，这种方法优于单独使用共享私钥的显式策略，因为这样增加了一些特定于数据包的数据，应该使对方更难于破解。同时可以把RC4看成一个一元输入和一元输出的设备，输入端输入的是有限位的初始密钥，输出端输出的是连续不断的密码流。如果攻击者只获取到输出密码流，其并不能计算出初始密钥。



图2-1-2 WEP加密过程

以WEP-40（64位加密）来解释加密过程：24位的初始化向量IV和40位密钥（WEP Key）串联成64位的初始密钥（Seed），把这个初始密钥作为输入，进行RC4运算，产生了一连串的密钥流（Key Stream）。把我们要传输的明文数据（Plaintext）和根据它算出来的32位检验值（CRC-32）进行串联，再把串联后的结果和RC4算法产生的密码流进行基于位的异或运算得到的密文数据（Ciphertext）。然后把IV作为“头部”置于密文数据前。这就是整个加密模型的流程。



图2-1-3 WEP解密过程

在数据包传输过程中，接收方和发送方有相同的WEP Key，接送方从数据包中提取出IV值就可以进行运算得到和发送方相同的初始密钥（Seed），因此经过RC4编码可以产生相同的Key Stream，将Key Stream和密文数据进行异或比特运算，可以得到明文数据（Plaint Text）。

如图所示，运算结果是明文P，这样接收端就可以收到来自发送端的数据了。虽然其他用户也可以看到IV，但因为不知道密钥K，所以不知道密钥流RC4(IV,K)，因此无法从密文C中计算出明文P来。

**2.2 WEP加密模型安全性分析**

对WEP加密模型进行攻击的手段一般有两种方式。一种是共享密钥攻击：攻击者通过侦听用户流量或者入侵用户网络等方法，窃取用户的共享密钥，从而对WEP进行攻击。如果用户在设定的时候选择共享密钥认证，进行一种质询—响应机制，那么攻击者可以伪装成合法用户进行攻击。但是共享密钥泄漏并不是WEP攻击的最主要手段。

WEP攻击的另一种方法是由于WEP标准设定的时候，设计工程师对WEP标准方面参数设定的不合理的选择，在一些参数的选择上，WEP有着一些差强人意的设计，攻击者会利用参数漏洞进行攻击。

WEP设计标准在加密方面存在以下弊端。

1. WEP加密和解密模型使用的是RC4算法。RC4算法不是一个不可破解的算法，RC4算法本身就有不严谨的地方，攻击者可以利用这个漏洞对WEP进行攻击。

2. WEP模型设定标准的时候对于同一个AP来说，初始化向量IV是有限的，所以设定初始化向量IV是可以重复使用的，这样来说攻击者会使用相同密文和明文重复进行分析，这是WEP设计的一个缺陷。WEP协议在制定的时候也没有规定每个数据包的IV值要怎样设定，有些设备在每次和对端连接后的每一个IV值是从0开始，然后每发一个数据包IV值就增加1，这样小IV值的重复利用频率就更高了。当攻击者捕捉到两个使用相同IV值的密文C1和C2后，它可以做下面的运算：

IF C1 = P1 ⊕ RC4(IV,K)

AND C2 = P2 ⊕ RC4(IV,K)

THEN C1 ⊕ C2 = (P1 ⊕ RC4(IV,K)) ⊕ (P2 ⊕ RC4(IV,K)) = P1 ⊕ P2

两个密文的异或运算结果为两个明文的异或运算，如果攻击者知道了两个明文中的一个，如P1，那么他就可以通过公式计算出另外一个明文P2。知道其中一个明文，基于这个IV值的RC4(IV,K)也可以计算出来。

3. WEP设计标准不提供自动修改密钥。因此，当用户修改密钥的时候需要用户手动对接入点AP工作站进行重新设置密钥，这样给用户的安全防护带来隐患，攻击者可以利用流量统计和破解密钥的方法进行被动攻击。

4. WEP设计标准认证协议是单向认证的，这认证方式过于简单，不能有效地进行访问控制。

5. WEP设计引入综合检测值ICV来提供对数据完整性的保护，但是完整性保护只应用于数据载荷，没有保护源，目的地址和防止重放等，ICV是一个32位的CRC32的数值，而CRC32设计函数是用来检查消息中的随机错误的，并不是安全杂凑函数，不具有身份认证能力，无法抵御对明文的篡改。

3 TKIP加密模型及其安全性分析

**3.1 TKIP加密模型**

TKP（Temporal Key Integrity Protocol）是一种“半新”的加密协定。因为TKIP保留了WEP所使用的加密引擎RC4和WEP的基本架构，这样的保留是为了要使TKIP能够兼容WEP的硬件，以便于使用者日后升级。TKIP原本被称为WEP2，但由于WEP经证实存在瑕疵，为了能与WEP有所区别，因此更名为TKIP。

WEP模型最大的弱点在于过短的IV以及直接以使用者设定的WEP密钥为输入，产生密钥串流，再结合消息进行加密。TKJP与WEP一样基于RC4加密算法，且对现有的WEP进行了改进，在现有的WEP加密引擎中增加了“密钥细分（每发一个包重新生成一个新的密钥）”、“消息完整性检查（MIC）”、“具有序列功能的初始向量”和“密钥生成和定期更新功能”等4种算法，提高了加密安全强度。TKIP将24-bit的IV增加为48-bit，可以有效防止IV矢量空间在密钥的使用期限内耗尽。在TKIP中，RC4用来产生密钥串流的密钥，是以混合密钥（Key Mixing）的方式产生的。首先无线网卡和AP之间在验证阶段或重新验证阶段随机协商出成对主密钥PMK，此PMK的任务之一就是要派生出暂时密钥TK，并于发送密钥时对密钥进行再加密。TKP再以暂时密钥以及其他元素（如发送端的MAC Address）作为输入，进行二个阶段的混合密钥程序产生出的密钥，这个密钥就是用来产生密钥串流的种子。因为使用混合密钥的方式，使得TKIP能为每一个传送的信息拥有自己单独的密钥。



图3-1-1 TKIP加密过程

如上面的加密算法，TA（传输地址）也就是发送者和接收者的MAC地址，TK（临时密钥）是基础密钥，TSC（传输序列计数器）是所谓的包序列号。这三个值通过阶段1和阶段2的混合作为WEP种子(seed),通过RC4运算后得到密码流进行加密。解密过程和加密过程相似。

**3.2 TKIP加密模型安全性分析**

TKIP中密码使用的密钥长度为128位。这解决了WEP的一个安全问题：过短的密钥长度。TKIP的一个重要特性是它变化每个数据包所使用的密钥。这就是它名称中“动态”出处。密钥通过将多种因素混合在一起生成，包括基本密钥（即TKIP中所谓的成对瞬时密钥）、发射站的MAC地址以及数据包的序列号。混合操作在设计上将对无线站和接入点的要求减少到最低程度，但仍具有足够的密码强度，使它不能被轻易破译）。

利用TKIP传送的每一个数据包都具有独有的48位序列号，这个序列号在每次传送新数据包时递增，并被用作初始化向量和密钥的一部分。将序列号加到密钥中，确保了每个数据包使用不同的密钥。这解决了WEP的一个问题，即所谓的“碰撞攻击”。这种攻击发生在两个不同数据包使用同样的密钥时。在使用不同的密钥时，不会出现碰撞。

以数据包序列号作为初始化向量IV，还解决了隐患问题，即所谓的“重放攻击（Replay Attacks）”。由于48位序列号需要数千年时间才会出现重复，因此没有人可以重放来自无线连接的老数据包：由于序列号不正确，这些数据包将作为失序包被检测出来。

被混合到TKIP密钥中的最重要因素是基本密钥。如果没有一种生成独特的基本密钥的方法，TKIP尽管可以解决许多WEP存在的问题，但却不能解决最糟糕的问题：所有人都在无线局域网上不断重复使用一个众所周知的密钥。为了解决这个问题，TKIP生成混合到每个包密钥中的基本密钥。无线站每次与接入点建立联系时，就生成一一个新基本密钥。这个基本密钥通过将特定的会话内容与用接入点和无线站生成的一些随机数以及接入点和无线站的MAC地址进行散列处理来产生。由于采用802.1x认证，这个会话内容是特定的，而且由认证服务器安全地传送给无线站。

TKIP是基于WEP的，仍然使用RC4算法，但具有新的特征，并针对WEPd漏洞进行了改进，增加了4个新的特性：（1）加密信息完整性代码，即MIC/MAC，防止非法用户对信息体的篡改和伪造；（2）建立单包密钥构建机制（per-packet key construction），免除了IV与弱密钥的相关性，防止针对弱密钥的攻击；（3）扩展的48位IV和IV顺序规则，防止重放攻击；（4）密钥重新获取和分发机制，防止因密码碰撞受到攻击。

通过以上的分析可知，TKIP的设计提高了整个系统的安全性，它针对WEP的缺陷，提出了相应的补救措施。并且，在TKIP的过程中，除了最后的WEP加密之外，前面的部分属于软件升级，这样实现了现存资源上可能到达的最大安全性。

4 CMCC加密模型及其安全性分析

**4.1 CMCC加密模型**

CCMP是基于AES的CCM模式，AES是美国NIST制定的替代DES的新一代分组加密算法，所有在CCMP中用到的AES处理都使用一个128位的密钥和一个128位大小的数据块，AES标准汇聚了强安全性、高性能、高效率、易用和灵活等优点，非常适合于各种计算环境下的软硬件实现。CCM是一种通用的模式，它可以使用在任何成块的加密算法中。CCM模式使用计数模式（CTR）提供数据保密，并采用密码区块链信息认证码（CBC-MAC）来提供数据认证和数据完整性服务。CCMP是802.11i强制使用的加密方式，是WLAN安全长远的解决方案，为WLAN提供了加密、认证、完整性和抗重放攻击的能力，能解决WEP中出现的所有问题。

CCMP是另一种提供数据保密性和完整性的封装协议。图4-1-1和图4-4-5分别给出了CCMP加密和解密的流程。



图4-1-1 CCMP加密过程



图4-1-2 CCMP解密过程

CCMP算法加密步骤如下：

（1）为了使每个MPDU都使用新的、不同的的数据包序号（PN），PN将在加密不同包时递增，这样对于同样的临时密钥，PN将不会重复。需要注意的是，重传的MPDU的PN不会改变。

（2）利用MPDU的头部（也就是MAC的头部）为CCM生成附加认证数据（AAD）。CCM为AAD中的字段提供完整性保护。

（3）以PN、地址A2（MPDU中的发送地址）和MPDU的优先级Priority来构建CCM的现时Nonce。

（4）利用新的PN和密钥标识符KeyID来建立CCMP头部（密文MPDU的前8个字节）。

（5）以附加认证数据AAD、现时Nonce以及MPDU数据为输入，在临时密钥TK的控制下进行AES-CCM加密，得到密文数据和消息完整性代码MIC。

（6）将CCMP头、明文MAC头、密文数据以及MIC串接在一起，组合成一定格式的密文MPDU，然后发送密文MPDU。

CCMP算法解密步骤如下：

（1）分析接收到的密文MPDU，提取MAC头、MIC、A2、优先级、PN和密文数据部分。

（2）以MAC头构建附加认证数据AAD，以A2、优先级和PN构建现时Nonce。

（3）以附加认证数据AAD、现时Nonce、密文数据以及消息完整性代码MIC为输入，在临时密钥TK的控制下进行AES-CCM解密，恢复出明文数据，并且进行MIC检查，如果发现数据被篡改，则抛弃当前数据。

（4）将MAC头和明文数据连接成一个完整的明文MPDU，并通过比较MPDU中的PN和会话中所维护的接收到的PN的大小来进行重放攻击检查，若为重放则抛弃该帧，若重放检查无误，则将该明文MPDU帧送往上一层处理。

**4.2 CMCC加密模型安全性分析**

CCMP基于AES分组密码算法，使用CCM操作模式。CCM模式是保护机密性的计数器模式（CTR）和进行完整性校验的密码区块链信息认证码模式（CBC-MAC）的合成。这两种模式都有着相当长时间的研究，有着良好的易于理解的密码属性，提供了很高的安全性并且在软件和硬件上都有着良好的表现。

对于CTR模式和CBC-MAC模式来说，使用的密钥是相同的。尽管对于同一密钥用于不同的功能可能会引起安全上的问题，但是由于CTR模式和CBC-MAC模式分别构造不同的IV，20多年的密码实践证明在这种特殊情况下，不会产生安全问题。使用一个密钥的好处是简化CCM的设计，降低了对密钥管理的要求，从而减少了因用户误用或密钥管理不健全所造成的安全漏洞。

CCM对于每一次会话都假设一个新的临时密钥，并且采用单增计数器产生的48位包序列号（PN）防止重放攻击，接收方采用抗重放窗口检测收到的数据包是否在合法范围内。

总体而言，CTR和CBC-MAC在密码实践中都证明是安全的，CCMP是健壮的数据保密协议，目前尚未发现任何安全上的问题。

5 总结

IEEE 802.11i标准针对以往WLAN加密机制的各种缺陷做了很大程度上的改进，TKIP协议在一定程度上可以提高原有WEP协议的安全性，其安全强度提高4个数量级，但并不能从根本上解决问题，只有早日应用CCMP封装协议才能实现健壮的数据保密。但是采用CCMP就需要采用全新的网络硬件和软件，势必造成已有设备的浪费。因此，如何在满足安全性要求和硬件档次要求、执行效率高低、保密费用与数据敏感性之间进行权衡，是需要进一步研究的问题。