无线局域网产品工程化实现指南
第8部分：WAPI与IEEE 802.11ac

A Guide to Wireless Local Area Network Product Engineering Implementation -- Part 8: WAPI & IEEE 802.11ac

2016-03-01发布 2016-03-01实施
版权声明

本文件版权归WAPI产业联盟（中国计算机行业协会无线网络和网络安全接入技术专业委员会）所有。

本文件以电子文档形式面向公众公开。本声明在此授权所有组织或者个人对本文件进行使用和复制。任何组织或者个人对本文件的修改、翻译、摘编、汇编、销售行为，应事先获得WAPI产业联盟书面授权，否则视为侵权。

联系WAPI产业联盟标准部门（lmbz@wapia.org）可获取本文件授权相关信息。
目次

前言 .......................................................................................................................... III
引言 ............................................................................................................................ IV
1 范围 ....................................................................................................................... 1
2 规范性引用文件 .................................................................................................... 1
3 缩略语 ................................................................................................................... 1
4 IEEE802.11ac 数据帧格式与 WAPI 使用的数据帧格式的变化对比 .................. 2
5 WPI 的 A-MSDU 的封装 .................................................................................... 3
6 WPI 的 A-MPDU 的封装 .................................................................................... 4
7 GCM-SM4 的支持 .................................................................................................. 5
7.1 GCM-SM4 工作模式支持 ................................................................................ 5
7.2 封装与解封装 ................................................................................................... 5
7.3 Key 的使用规则 .................................................................................................. 8
7.4 数据分组序号 PN 的使用规则 ......................................................................... 8
附录 A（资料性附录） WAPI .............................................................................. 9
附录 B（资料性附录） IEEE802.11ac .................................................................. 10
附录 C（资料性附录） GCM 工作模式介绍 .......................................................... 11
C.1 128 比特分组密码的 GCM 加密及工作模式简单介绍 .................................. 11
C.2 128 比特分组密码的 GCM 解密及工作模式简单介绍 .................................. 12
C.3 GCM-SM4 测试用例 ....................................................................................... 12
前言

本技术规范由WAPI产业联盟和工业和信息化部宽带无线IP标准工作组共同提出，由中国电子技术标准化研究院、中国电子技术标准化研究所归口。

本技术规范起草单位：WAPI产业联盟“无线局域网产品工程化实现指南产品方案组”暨工业和信息化部宽带无线IP标准工作组“无线局域网产品工程化实现指南标准项目组”（西安西电捷通无线网络通讯股份有限公司、无线网络安全技术国家工程实验室、广州杰赛科技股份有限公司、中国电子技术标准化研究院、国家无线电监测中心检测中心、北京傲天动联技术有限公司、重庆邮电大学、北京邮电大学、桂林电子科技大学、无锡中太数据通信有限公司、北京五龙电信技术公司、北京登合科技有限公司、宇龙计算机通信科技（深圳）有限公司、北京六合万通微电子技术股份有限公司、深圳市华胜科技有限公司）。

本技术规范主要起草人：胡亚楠、童伟刚、师倩俊、徐冬梅、朱跃生、杨峰、陈康先、龙昭华、仇洪冰、韦安营、韦慧、刘鹄、田辉、黄剑明、高宏、皮永平、陈维刚、苑克龙、寿国梁、王海永、李建国、单丹、刘彬、李翔。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。
无线局域网鉴别与保密基础结构WAPI（wireless local area network authentication and privacy infrastructure）为无线局域网中的数据链路层提供了安全解决方案，包括身份鉴别、密钥管理、数据加密、数据鉴别和重放保护等功能。IEEE 802.11ac的核心技术主要基于IEEE 802.11a，继续工作在5.0GHz频段上以保证向下兼容性，但数据传输通道会大大扩充，在当前20MHz的基础上增至40MHz或者80MHz，甚至有可能达到160MHz。标准的理论传输速度最高有望达到1Gbps。

虽然以上的两种方案分别涉及不同的领域，但是它们之间并不存在直接的矛盾或冲突，是可以相互结合、互为补充的。WAPI与IEEE802.11ac的基本介绍参见附录A和B。

WAPI与IEEE802.11ac的结合遵循以下基本原则：

a) 无线局域网中的非安全方案使用IEEE802.11ac；
b) 无线局域网中安全方案完全使用WAPI机制；
c) 无线局域网中数据传输保护的安全方案由WPI保密基础结构与IEEE802.11ac的帧封装技术结合而成。
无线局域网产品工程化实现指南

第8部分 WAPI与IEEE802.11ac

1 范围

本指导性技术文件规定了WAPI与IEEE802.11ac融合的工程化实现的关键问题说明，主要为使用WAPI且支持IEEE802.11ac快速传输的功能。

本指导性技术文件适用于WAPI与IEEE802.11ac标准融合的工程化实现的应用。

2 规范性引用文件

下列文件中的条款通过本指导性技术文件的引用而成为本指导性技术文件的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本指导性技术文件，然而，鼓励根据本指导性技术文件达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本指导性技术文件。

GB 15629.11-2003/XG1-2006 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范 第1号修改单
IEEE Std 802.11ac-2013 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范 补篇 4：6 GHz频带以下吞吐量的增强
IEEE Std 802.11-2012 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范 第11部分：无线局域网媒体访问控制和物理层规范

3 缩略语

下列缩略语适用于本指导性技术文件：

AP 接入点（Access Point）
A-MPDU MPDU聚合（aggregate medium access control (MAC) protocol data unit）
A-MSDU MSDU聚合（aggregate medium access control (MAC) service data unit）
GCM 伽罗瓦计数器模式（Galois/Counter Mode）
GCM-SM4 伽罗瓦计数器模式和SM4分组密码算法
HT 高吞吐量（High-throughput）
MPDU MAC协议数据单元（medium access control (MAC) protocol data unit）
MSDU MAC服务数据单元（medium access control (MAC) service data unit）
PLCP 物理层会聚处理（physical layer convergence procedure）
PPDU 物理层协议数据单元（PLCP protocol data unit）
PSDU 物理层服务数据单元（PLCP service data unit）
QoS 服务质量（Quality of Service）
SM4 SM4分组密码算法，等同于SMS4分组密码算法
STA 端站（Station）
VHT 超高吞吐量（Very High throughput）
WAI 无线局域网鉴别基础结构（WLAN Authentication Infrastructure）
WAPI 无线局域网鉴别与保密基础结构（WLAN Authentication and Privacy Infrastructure）
WPI 无线局域网保密基础结构（WLAN Privacy Infrastructure）
4 IEEE802.11ac 数据帧格式与 WAPI 使用的数据帧格式的变化对比

图 1 是 IEEE802.11ac 帧格式。

<table>
<thead>
<tr>
<th>Frame Control</th>
<th>Duration/ID</th>
<th>Address 1</th>
<th>Address 2</th>
<th>Address 3</th>
<th>Sequence Control</th>
<th>Address 4</th>
<th>QoS Control</th>
<th>HT Control</th>
<th>Frame Body</th>
<th>FCS</th>
</tr>
</thead>
</table>

图 1 IEEE802.11ac 帧格式

而 WAPI 使用的无线数据帧格式 MAC header 里没有出现对 HT Control 子字段的说明。此字段会出现在相应地 QoS 数据和管理帧里。所以需要将 WAPI 使用的无线帧帧头与 IEEE802.11ac 统一。

即 WAPI 涉及到的无线数据帧的帧头格式与 IEEE802.11ac 保持一致。

如上帧头的使用，导致了 WPI-SM4 的 MPDU 封装结构和完整性校验数据都有相应的变化。改变如下：
1) WPI-SM4 的 MPDU 封装结构

其中：
——MAC 头字段，当地址 4 存在时，长度为 30 个八位位组；当地址 4 不存在时，长度为 24 个八位位组。当 MAC 头包含服务质量控制子字段时，长度再增加两个八位位组。如果 MAC 头再包含了 HT Control 子字段，则长度再增加四个八位位组。

WPI-SM4 的 MPDU 封装结构的其他部分与 WAPI 一致。

2) 完整性校验数据

其中：完整性校验数据包含两部分内容：
第一部分：
——帧控制（比特 4、5、6、11、12、13 置为 0，比特 14 置为 1）：2 个八位位组；
——地址 1：6 个八位位组；
——地址 2：6 个八位位组；
——序列控制（比特 4~15 置为 0）：2 个八位位组；
——地址 3：6 个八位位组；
——地址 4：6 个八位位组；若 MAC 帧头中不存在地址 4，则该字段的 6 个八位位组的值均置为 0；
——服务质量控制：2 个八位位组：若 MAC 帧头包含服务质量控制字段，则该字段存在，比特 4~15 置为 0（如果 STA 和对端的 PAP A-MSDU 能力域为 1，比特 7（A-MSDU Present 域）用于构建完
完整性校验数据)，其它字段与MAC帧头中包含的服务质量控制字段取值相同：
——KeyIdx：1个八位位组；
——保留：1个八位位组；
——L：2个八位位组，该字段表示PDU数据的长度，按照大数结尾编码计算。
第二部分：
——PDU数据：大于0个八位位组。
在计算完整性校验码MIC时需要使用的字段中，没有特意强调取值的比特位，应使用当前值进行MIC计算。

5 WPI的A-MSDU的封装

A-MSDU子字段结构如图4所示。与其他标准相比较，只是MSDU的长度有变化。

<table>
<thead>
<tr>
<th>目的地址DA</th>
<th>源地址SA</th>
<th>长度L</th>
<th>MSDU</th>
<th>填充</th>
</tr>
</thead>
<tbody>
<tr>
<td>6个八位位组</td>
<td>6个八位位组</td>
<td>2个八位位组</td>
<td>变长八位位组</td>
<td>0-3个八位位组</td>
</tr>
</tbody>
</table>

图4 A-MSDU子字段结构

一个A-MSDU由一序列的A-MSDU子字段组成，每个A-MSDU子字段包括了一个A-MSDU头及0-3个八位位组的填充，便于它的长度是4个八位位组的整数倍。最后一个A-MSDU子字段不需要填充。A-MSDU封装格式如图5所示。

WPI的A-MSDU封装格式如图6所示。
### 6 WPI 的 A-MPDU 封装

A-MPDU 子字段结构如图 7 所示。与其他标准相比较，MPDU 分隔符，后面的填充有变化。

一个 A-MPDU 由一序列的 A-MPDU 子字段组成。每个 A-MPDU 子字段包括了一个 A-MPDU 分隔符，后面可选跟着一个 MPDU。在一个 A-MPDU 里每个非最后一个 A-MPDU 子字段都要填充必要的字节，便于它的长度是 4 个八位位组的整数倍。在 VHT PPDU 里，最后一个 A-MPDU 子字段也要填充，而在 HT PPDU 里，最后一个 A-MPDU 子字段不需要填充。

A-MPDU 封装格式如图 8 所示。
WPI 的 A-MPDU 封装格式如图 9 所示。

![WPI 的 A-MPDU 封装格式](image)

图 9 WPI 的 A-MPDU 封装格式

7 GCM-SM4 的支持

7.1 GCM-SM4 工作模式支持

WPI 保密基础结构对 MAC 子层的 MPDU 进行加、解密处理，但对于 WAI 协议分组不进行加解密处理。

GCM-SM4 密码套件中采用的分组密码算法为 SM4。GCM 的工作模式与国际标准保持一致。参见附录 C。使用的 GCM-SM4 密码套件如表 1 所示：

<table>
<thead>
<tr>
<th>OUI</th>
<th>类型</th>
<th>含义</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-14-72</td>
<td>0</td>
<td>保留</td>
</tr>
<tr>
<td>00-14-72</td>
<td>1</td>
<td>WPI-SM4</td>
</tr>
<tr>
<td>00-14-72</td>
<td>2</td>
<td>WPI-GCM-SM4</td>
</tr>
<tr>
<td>其他</td>
<td>3~255</td>
<td>保留</td>
</tr>
</tbody>
</table>

7.2 封装与解封装

WPI-GCM-SM4 的 MPDU 封装结构如下：

![WPI-GCM-SM4 的 MPDU 封装结构](image)

图 10 WPI-GCM-SM4 的 MPDU 封装结构

其中：
——MAC 头字段，当地址 4 存在时，长度为 30 个八位位组；当地址 4 不存在时，长度为 24 个八位位组。当 MAC 头包含服务质量控制子字段时，长度再增加两个八位位组。如果 MAC 头再包含了 HT Control 子字段，则长度再增加四个八位位组。
——KeyIdx 字段长度为 1 个八位位组，表示 USKID 或 MSKID 或 STAKeyID 值。
——保留字段长度为 1 个八位位组，默认值为 0。
——PN 字段长度为 16 个八位位组，表示一个整数，标识数据分组序号，数据分组序号 PN 字段按照小数结尾编码发送。该数据分组序号低 96 比特作为 GCM 模式下数据加密时所需的 IV。PN...
的使用规则及实例参见7.4节。
——PDU（数据）字段为MPDU数据，最大长度为2278=2312−18(WPI头)−16(Auth Tag)。
——Auth Tag字段长度为16个八位位组。
——FCS字段长度为4个八位位组，为MAC帧格式的帧校验序列。

Additional authenticated data (AAD)结构组成参见《无线局域网工程化实现指南第1部分 WAPI与IEEE802.11n》中的完整性校验数据的第一部分的定义，结构中各个部分的使用说明除以下描述之外与之完全相同。

✔ QC如果出现，其是表示MSDU优先级的2个字节的QoS Control字段。如果在non-DMG BSS里STA和对端的SPP A-MSDU Capable字段都为1，那么AAD构建里使用比特7（the A-MSDU Present字段）。当STA或对端的SPP A-MSDU Capable字段为0, QC字段的其余比特设置为0（比特4-6, 8-15，比特7）。

数据发送时，GCM-SM4的MPDU封装方框图如下：

数据发送时，GCM-SM4封装与输入参数的映射关系如图12描述：

数据发送时，GCM-SM4使用下面的规则对MPDU进行封装：
a) 增加PN，每个MPDU都使用不相同的PN，重传时PN不改变
b) 使用MPDU头里的字段构造GCM使用的AAD。GCM算法提供了AAD里字段的完整性保护。如果当重传时MPDU头里某些字段发生改变，那么在构造AAD时将其屏蔽设置为0

c) 根据PN的低96比特作为IV构造Counter，PN的使用规则及实例参见7.4节

d) 将新的PN和Keyid放在WPI头里

e) GCM加密处理过程使用Key，AAD，Counter和MPDU数据生成密文和MIC。此处可以参考附录C的GCM-SM4加密模式

f) 原始的MPDU头，WPI头和加密后的MPDU数据及MIC形成了加密MPDU

数据接收时，GCM-SM4的MPDU解封装方框图13如下：

数据接收时，GCM-SM4解封装与输入参数的映射关系如图14描述：

数据接收时，GCM-SM4使用下面的规则解密MPDU密文数据，并对MPDU明文进行解封装：

a) 分解MPDU密文，构建AAD和Counter

b) 通过MPDU密文的MPDU头形成AAD

c) PN字段低96比特作为IV构建Counter，PN的使用规则及实例参见7.4节

d) MIC被提取出来用于GCM完整性校验

e) GCM接收过程使用Key，AAD，Counter，MIC和MPDU密文数据这些参数进行处理，得出MPDU明文数据，同时也校验了AAD和MPDU明文数据的完整性。此处可以参考附录C的GCM-SM4解密模式
f) MPDU头和MPDU明文数据可能需要连接在一起形成一个明文MPDU

g) 解密过程通过比较MPDU里的PN是不是要大于重放计算数来防止MPDU重放攻击

7.3 Key的使用规则

GCM-SM4采用单播加密密钥UEK作为GCM数据接收和数据发送时使用的Key, 即单播会话密钥的第一个16个八位位组。详见GB 15629.11-2003/XG1-2006第一号修改单。

7.4 数据分组序号PN的使用规则

数据分组序号PN与GB 15629.11-2003/XG1-2006第一号修改单中定义的数据分组序号PN使用规则相同, GCM-SM4里将PN的低96比特作为IV使用。当PN的低96比特溢出, 更新密钥。

如PN值0x5c365c365c365c365c365c365c365c36, 使用低96比特构造的IV, 如图15所示:

<table>
<thead>
<tr>
<th>PN:</th>
<th>5C</th>
<th>36</th>
<th>5C</th>
<th>36</th>
<th>...</th>
<th>5C</th>
<th>37</th>
</tr>
</thead>
<tbody>
<tr>
<td>IV:</td>
<td>5C</td>
<td>36</td>
<td>...</td>
<td>5C</td>
<td>37</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

图15 IV构造实例1

如PN值0x5c365c365c365c365c365c365c365c36, 使用低96比特构造的IV, 如图16所示:

<table>
<thead>
<tr>
<th>PN:</th>
<th>5C</th>
<th>36</th>
<th>5C</th>
<th>36</th>
<th>...</th>
<th>5C</th>
<th>37</th>
</tr>
</thead>
<tbody>
<tr>
<td>IV:</td>
<td>5C</td>
<td>36</td>
<td>...</td>
<td>5C</td>
<td>36</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

图16 IV构造实例2
无线局域网鉴别与保密基础结构WAPI（wireless local area network authentication and privacy infrastructure）是用于提供无线局域网中的身份鉴别和数据机密性的安全机制，由无线局域网鉴别基础结构（WAI）和无线局域网保密基础结构（WPI）组成。其中：

—— WAI（WLAN authentication infrastructure）是用于无线局域网中身份鉴别和密钥管理的安全方案；
—— WPI（WLAN privacy infrastructure）是用于无线局域网中数据传输保护的安全方案，包括数据加密、数据鉴别和重放保护等功能。

注：关于WAPI安全机制的详细内容参见GB 15629.11-2003/XG1-2006。
IEEE 802.11ac 标准在现有 IEEE802.11 标准基础之上对 MAC 层协议进行改进，使 WLAN 系统能够支持更高速的传输。这个补篇主要增加了以下内容：
—— 帧格式（帧头）格式上有变化
—— A-MSDU 和 A-MPDU 格式上有变化
C.1 128 比特分组密码的 GCM 加密及工作模式简单介绍

1. GCM 输入参数
   - 合适长度的密钥 Key。
   - GCM 的一个重要特点是 initialization vectors (IV) 可以根据需要指定 1 到 $2^{64}$ 个比特的长度。
   - 明文 P 可以是 0 到 $2^{32}$−256 个字节的长度。
   - Additional authenticated data (AAD) 认证数据简写为 A。这个数据不被加密，计算认证标签时使用。可以是 0 到 $2^{64}$ 个字节的长度。

2. GCM 两个输出简单介绍
   - 密文 C 的长度与明文长度一致
   - authentication tag 认证标签 T 长度可以是 0 到 128 个字节。这里指定 tag 的长度为 128 个字节即 16 个八位位组

3. GCM 加密操作过程

![GCM 加密过程图](image)

图1 GCM 加密过程
为简单起见，在上图中只有一个AAD分组，标识为Auth Data1，和两个明文数据分组。

- Counter 值：
  
  Counter 0 = IV | 0^{31} \mod 2^{32}

  Counter 1 = IV | (0^{31} + 1) \mod 2^{32}

  Counter i = IV | (0^{31} + i) \mod 2^{32}

- $E_K$ 分组密码算法
- Auth Data 根据需要构建

C.2 128 比特分组密码的GCM解密及工作模式简单介绍

1. 输入输出参数简单介绍
   - GCM 解密有 5 个输入参数：K, IV, C, A, 和 T
   - GCM 解密有 1 个输出：P

2. GCM 解密操作过程

   ![GCM 解密过程图](image)

   图 2 GCM 解密过程

C.3 GCM-SM4 测试用例
加密测试用例:

<table>
<thead>
<tr>
<th>参数名称</th>
<th>参数数据</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key(16)</td>
<td>00 01 00 02 00 03 00 04 00 05 00 06 00 07 00 08</td>
</tr>
<tr>
<td>IV(12)</td>
<td>5c 36 5c 36 5c 36 5c 36 5c 36 5c 36 5c 36</td>
</tr>
<tr>
<td>AAD(23)</td>
<td>ff ff ff ff ff ff 00 03 7f ff ff fe 89 2c 38 00 00 5c 36 5c 36 5c 36</td>
</tr>
<tr>
<td>P(48)</td>
<td>08 06 00 01 08 00 06 04 00 01 00 03 7f ff fe c0 a8 14 0a 00 00 00 00 00 00 0c 00 00 00 00 00 00</td>
</tr>
<tr>
<td>输出数据</td>
<td>C(48)</td>
</tr>
<tr>
<td>C(48)</td>
<td>0a 59 91 a6 70 dc 0e a2 6f 84 e4 55 a1 c0 61 47 8a a0 9f 2f be 90 49 46 29 bc 58 e7 5b e5 e9 1d bc 6d 21 49 bc 1f ba ca ca a9 72 2d 61 0f de 1d</td>
</tr>
<tr>
<td>tag(16)</td>
<td>99 20 b1 eb fb 59 02 5f 0e ba 77 8c f5 9a 5c c8</td>
</tr>
</tbody>
</table>

解密测试用例:

<table>
<thead>
<tr>
<th>参数名称</th>
<th>参数数据</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key(16)</td>
<td>00 01 00 02 00 03 00 04 00 05 00 06 00 07 00 08</td>
</tr>
<tr>
<td>IV(12)</td>
<td>5c 36 5c 36 5c 36 5c 36 5c 36 5c 36 5c 36</td>
</tr>
<tr>
<td>AAD(23)</td>
<td>ff ff ff ff ff ff 00 03 7f ff ff fe 89 2c 38 00 00 5c 36 5c 36 5c 36</td>
</tr>
<tr>
<td>tag(16)</td>
<td>99 20 b1 eb fb 59 02 5f 0e ba 77 8c f5 9a 5c c8</td>
</tr>
<tr>
<td>C(48)</td>
<td>0a 59 91 a6 70 dc 0e a2 6f 84 e4 55 a1 c0 61 47 8a a0 9f 2f be 90 49 46 29 bc 58 e7 5b e5 e9 1d bc 6d 21 49 bc 1f ba ca ca a9 72 2d 61 0f de 1d</td>
</tr>
<tr>
<td>输出数据</td>
<td>08 06 00 01 08 00 06 04 00 01 00 03 7f ff fe c0 a8 14 0a 00 00 00 00 00 00 0c 00 00 00 00 00 00</td>
</tr>
</tbody>
</table>