第 34 卷 第 1 期 计 算 机 工 程 2008 年 1 月
Vol.34 No.1 Computer Engineering January 2008
·安全技术· 文章编号：1000—3428(2008)01—0181—03 文献标识码：A 中图分类号：TP393

基于集中式 WLAN 分离 MAC 架构的 TKIP 协议

刘立群[1,2]，火久元[2]，唐 鼎[1]，武文忠[2]
(1. 中国科学院声学所高性能网络实验室，北京 100080；2. 兰州大学信息科学与工程学院，兰州 730000)

摘 要：实现强健安全网络(RSN)是大规模部署安全无线网络的最佳选择。该文分析了集中式 WLAN 结构的特点，比较了分离 MAC 方式与其他方式的不同之处，研究了 TKIP 协议封装原理。给出一种新的分离 MAC 功能的方法，在集中式 WLAN 分离 MAC 架构下设计实现了暂时密钥完整性协议(TKIP)，描述了软件在嵌入式系统中的实现。对有待进一步解决的问题进行了讨论。

关键词：集中式 WLAN；分离 MAC；强健安全网络；暂时密钥完整性协议；CBC-MAC 计数模式协议

TKIP Based on Centralized WLAN Split MAC Architecture

LIU Li-qun [1,2], HUO Jiu-yuan[2], TANG Ding [1], WU Wen-zhong [2]
(1. High-performance Network Lab, Institute of Acoustics, Chinese Academy of Sciences, Beijing 100080;
2. School of Information Science & Engineering, Lanzhou University, Lanzhou 730000)

【Abstract】 It's optimal to implement a RSN in large deployments of secure wireless network. This paper analyzes centralized WLAN characteristics and compares split MAC with other architectures. TKIP encapsulation principles are researched. It gives a new method for split MAC and TKIP implementation scheme in the new centralized WLAN split MAC architecture, and depicts the implementation of software in embedded system, and some further problems to be resolved.

【Key words】 centralized WLAN; split MAC; Robust Security Network(RSN); Temporal Key Integrity Protocol(TKIP); Counter mode with Cipher block chaining Message authentication code Protocol (CCMP)

传统的自治式WLAN结构[1]因自身缺陷，已不适应大规模部署无线网络的局势。最新涌现出的集中式WLAN分离MAC架构[1]有效、合理地解决了大规模部署问题，成为目前研究的热点。被广泛应用的有线等效保密(WEP)[2-3]安全规范在设计上存在漏洞，严重威胁了WLAN的安全性。IEEE 802.11i 标准提出的强健安全网络(Robust Security Network, RSN)，支持暂时密钥完整性协议(Temporal Key Integrity Protocol, TKIP)和CBC-MAC计数模式协议(Counter mode with Cipher block chaining Message authentication code Protocol, CCMP)[4]两种保证数据机密性和完整性的机制，极大地提高了WLAN的安全等级。目前，实现RSN安全规范，已成为保证无线网络安全性的重要措施。

1 集中式 WLAN 分离 MAC 架构介绍

1.1 集中式 WLAN 结构的特点

在传统的自治式结构中，802.11 功能是由无线接入点提供的。这种结构的缺陷是：必须单独对接入点进行配置和控制，加大了管理费用；无法检测和缓解整个 WLAN 上拒绝服务的发生；如果某个接入点遭到破坏，安全就无法得到保证。

集中式WLAN结构是由WLAN设备厂商提出的。它具有分层结构，利用一个或多个称为接入控制器(AC)[1]的集中式设备对接入点进行管理。802.11 功能由接入点和集中式设备共同提供，这种结构的特点是：对整个WLAN系统采用集中的管理模式，统一实施业务流量控制、认证、加密和执行策略；将 802.11 功能实现在接入点和集中式设备之间，具有很好的管理性和扩展性；采用“轻量型接入点”[1]的方式，减少了管理功能和运营成本。

1.2 分离 MAC 方式与其他方式的比较

根据IEEE 802.11 MAC功能在网络实体上实现方法的不同，可以将集中式WLAN结构划分为本地 MAC方式、分离MAC方式和远程 MAC方式[1]。3 种方式如图 1 所示。

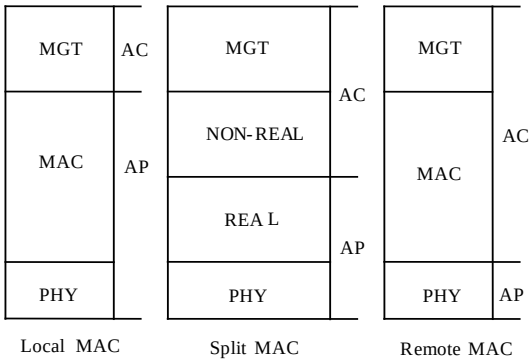

图 1 集中式 WLAN 结构的 3 种方式

本地 MAC 方式中，MAC 功能实现在 AP 上，AP 的配置和管理功能实现在 AC 上。这种方式实现简单，但 AP 的成本较高，AC 和 AP 存在功能上的重叠。

基金项目：中国下一代互联网示范工程 CNGI 基金资助项目“有线无线宽带统一接入控制器的研制 CNGI-iBAC”(CNGI-04-2-2D)
作者简介：刘立群(1982－)，女，硕士研究生，主研方向：网络计算，信息安全；火久元，工程师、硕士研究生；唐 鼎，助理研究员、博士；武文忠，副教授、博士
收稿日期：2007-01-15 **E-mail：**liulq04@lzu.cn

分离MAC方式是依据实时性的敏感度把MAC功能分别实现在 AP 和 AC 上。AP 支持无线网络的物理层和 MAC 层的实时性功能，AC 处理 MAC 层的非实时功能和高层服务。其优点是：减轻了 AP 负担，使得 AC 能够统一有效地管理大规模轻量型接入点，降低了 AP 的成本。但 IEEE802.11 标准对 MAC 功能的实时性并没有作明确规定，分离 MAC 没有统一的方案可循。

远程 MAC 方式目的是使 AP 尽量保持轻量级，只提供物理层功能，而 AC 提供所有的 MAC 功能。这种方式的 AP 功能简单，成本最低；但由于 MAC 的实时性功能实现在 AC 上，不利于开展时延敏感型业务。

综合比较这 3 种类型，分离 MAC 方式较其他 2 种方式提供更便利的管理模式，受到了大多数厂商的青睐。

2 TKIP 封装原理

IEEE802.11i标准中提出的RSN是一组定义了以下安全特性的BSS/ESS[4-7]：

(1)基于 802.1x[6-7]；

(2)接入点和站点间具有双向认证机制；

(3)具有密钥管理算法；

(4)动态的会话密钥；

(5)加强的数据包裹机制，包括 CCMP 和 TKIP 两种。

TKIP 是一个密码套件，是包裹在 WEP 外面的一套算法，它有效地解决了 WEP 的安全缺陷。相对于 WEP 来说，TKIP 增加了 4 种安全措施来增强安全性：新的初始化向量(IV)序列，消息完整码(MIC)，新的密钥混合函数，组密钥的分发和更新。

2.1 WEP 算法

WEP算法采用了在静态密钥中填入初始化向量的方法，把静态密钥转化成动态的伪随机密钥序列。完整性校验值(ICV)用来防止数据在传输过程中被篡改。RC4[2-3]序列加密算法是WEP的核心。

2.2 消息完整码

TKIP 使用消息完整码防止消息被篡改。TKIP 将 MIC 设计在 MSDU 层上，成功地阻断了在 MPDU 层上的攻击。TKIP 在待发送的数据分组 MSDU 上计算 MIC，MIC 被附加在 MSDU 有效载荷后。当 MSDU 达到可分段的长度时，TKIP 将其分段成一个或多个 MPDU。MPUD 作为 WEP 加密算法的明文输入。接收方把加密的 MPDU 组合得到 MSDU，在这个 MSDU 上检查 MIC 值是否有错误。如果 MIC 有错误，接收者将会丢弃它并触发相应的处理措施。

2.3 TKIP 的密钥生成与扩展

RSN网络定义了单播密钥和广播/组播密钥，分别通过 4 次握手协议和组密钥握手协议[4-7]得到。站点和接入点通过 4 次握手过程后，由PMK生成单播密钥(PTK)。PTK中有一部分是用于保护接入点和关联站点间单播通信安全的，称为TK。TK是TKIP的输入密钥，包括 3 部分[4-6]：

(1)用于加密数据包中有效载荷的密钥；

(2)用于计算发送 MIC 的加密密钥(TX MIC KEY)；

(3)用于计算接收 MIC 的解密密钥(RX MIC KEY)。

组密钥(GTK)是一个随机数，由接入点产生，用于保护接入点和关联站点间广播/组播通信的安全。TKIP 使用密钥混合函数将输入的 TK 扩展成更难破解的密钥序列，以提高 RC4 算法的安全性。

3 设计方案

3.1 MAC 功能的分离

本文采用集中式 WLAN 结构的分离 MAC 架构，并且实现 TKIP 保证机密性。这种架构是依据实时性的敏感度分离 MAC 功能的，实时性的功能没有明确定义，因此，本文总结分析了多数厂商采用的定义，结合 TKIP，对 RSN 的 MAC 功能给出了一种新的分割方法。把实时性的功能放在 AP 上实现，包括 Beacon 帧的产生、Probe 帧的发送和响应、控制帧的处理、同步处理等；把非实时的功能放在集中式设备中实现，包括 802.1x 认证、RSN 关联、RSN 重新关联、综合服务如 802.11 帧和 802.3 帧的转换、数据机密性 TKIP 封装协议、分段和组合。

3.2 方案实现的关键

集中式设备统一管理多个接入点，有效维护它们的信息以及关联站点的信息，是实现TKIP的关键。因此，本文建立了 2 个信息表：维护接入点信息的表WlanDevInfo和维护关联站点信息的表SibEntry。WlanDevInfo表项中包括了一个接入点的IP地址、BSSID、功率、信道、支持的认证类型、加密算法、用于组播通信的密钥以及关联站点的信息。SibEntry表项中包括了一个关联站点的MAC地址、状态、关联标识以及指向这个接入点的指针。

信息表的建立有利于处理和维护不同类型的密钥。在集中式 WLAN 结构中，建立关联的一对实体在单播通信时使用单播密钥，不同的站点使用不同的密钥。广播/组播通信时，接入点与一个组中的站点使用一致的组密钥，不同接入点使用不同的组密钥。因此，需要在上述信息表 WlanDevInfo 表项中添加组密钥，在 SibEntry 表项中添加单播密钥。

4 软件实现

宽带接入控制器(iBAC)位于各种接入网与 IP 核心网的衔接处，支持有线与无线接入用户，主要负责用户的接入认证和移动性管理。本方案实现了 iBAC 的子功能，用于提供安全的无线网络，iBAC 采用嵌入式系统，支持 TKIP 的软件实现在嵌入式系统的内核驱动中。

4.1 软件系统结构

软件完成了无线网络的数据转发以及数据机密性和完整性功能，系统结构如图 2 所示。

软件包括以下几个部分：

(1)物理以太网接口：AC 的一个以太网接口，由这个接口接收来自 AP 的数据。

(2)GRE 接收发送：提供 GRE 接收、GRE 发送接口。GRE 接收接口完成 GRE 数据包的解封装，并将 802.11 帧交给 AC 核心模块处理。GRE 发送接口将 802.11 帧封装在 GRE 数据包中并交给 TCP/IP 协议栈完成转发。

(3)管理帧处理：处理管理帧，对不同子类型的管理帧作出不同的响应。

(4)数据帧处理：处理数据帧。将数据帧送至 TKIP 模块处理。

(5)TKIP 处理：提供 TKIP 安全机制，用于封装/解封装数据帧，须从密钥维护模块中获得密钥。包括 MIC 计算校验、IV 设置、密钥混合函数(Phase1, Phase2)、WEP 加解密等子模块。

(6)密钥维护：通过 Netlink 消息接收密钥协商模块发送的密钥。判断密钥类型，将单播密钥添加到 SibEntry 中，组

密钥添加到 WlanDevInfo 中。

(7)AP 配置：通过 Netlink 消息接收 AP 设置模块发送的 AP 配置信息。

(8)虚拟以太网接口：是软件与协议栈的接口。功能包括将以太网帧转换成 IP 包交给协议栈处理以及将协议栈发送的 IP 包转换成以太网帧并交给 AC 核心模块处理。

(9)密钥协商模块和 AP 设置模块位于嵌入式系统的用户空间，分别提供 802.1x 认证、密钥协商功能以及设置 AP 信息等功能。

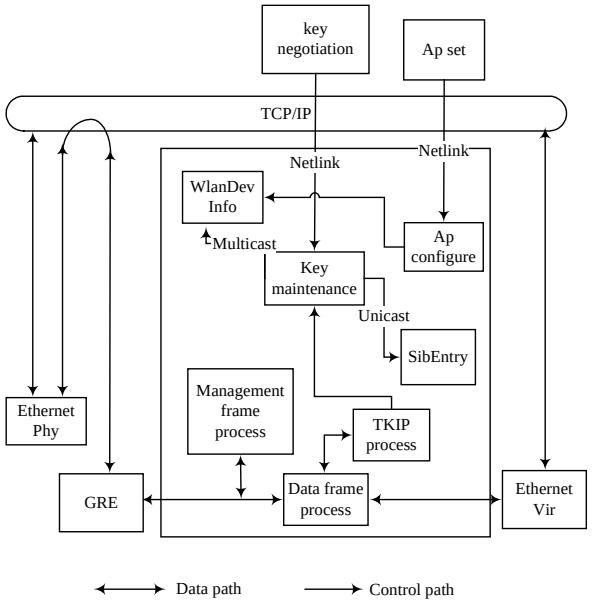

图 2　软件系统结构

4.2　软件运行流程

iBAC 中无线网络接收帧的流程以及 TKIP 解封装过程如图 3 所示。

接入点接收到帧，判断它是否为控制帧或子类型为 Probe request 的管理帧。如果是，接入点作出响应；否则，把它传送到嵌入式系统内核中。

当内核收到帧后，判断帧类型，若是数据帧，送至数据解封装子模块；若是管理帧，根据子类型作出响应，发送到协议栈。对于单播数据帧，从 SibEntry 中取得密钥；对于组播帧，从 WlanDevInfo 中取得密钥。将数据帧和密钥送至 TKIP 解封装子模块。TKIP 解封装是封装的逆操作。帧体是加密后的密文，通过 WEP 解密算法得到相应的明文。解封装完成后，需要进行重放攻击检查，查看 TSC，若返回错误，则作为失序帧丢弃；否则，将接收的多个分段 MPDU 组合后构造出 MSDU。根据密钥中的 RX MIC KEY，计算出 MSDU 的 MIC 值。判断它是否与 MSDU 中的 MIC 相等，若相等，则说明 MSDU 没有被篡改，发送至协议栈；否则，对它采取相应的处理措施。

本软件成功运行在 iBAC 上，性能良好，TKIP 保证了较好的数据机密性与完整性。

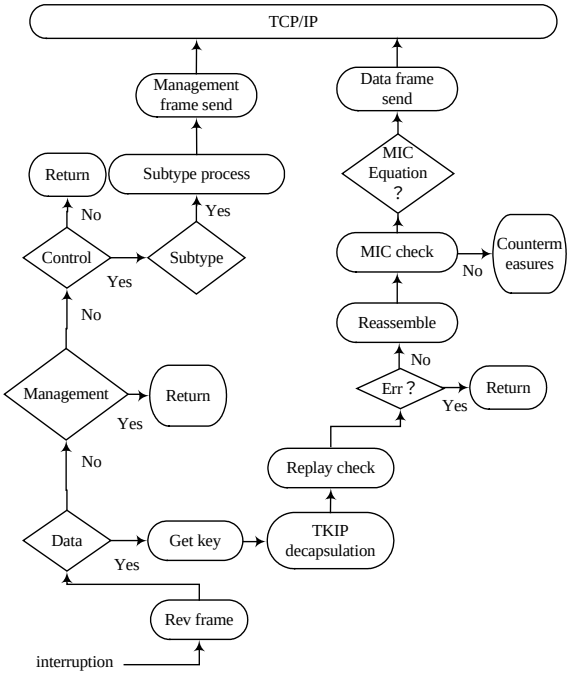

图 3　TKIP 解封装流程

5　结束语

在集中式 WLAN 结构中实现 RSN，是目前大规模部署安全的无线网络的一个趋势。本文给出了分割 MAC 功能的新方法，并在集中式设备中实现了 TKIP。但 TKIP 没有脱离 WEP 的核心，仍然存在安全隐患，只能作为一种暂时的机密性解决方案。RSN 强制实施的 CCMP 提供了强大的安全性，本方案有待于进一步实现 CCMP，以便提供更安全可靠的网络机制。

参考文献

[1] IETF. Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP)[S]. RFC 4118, 2005-06.

[2] IEEE Standard 802.11-1999 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications[S], 1999.

[3] 国家标准化管理委员会. GB15629.11-2003 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: 无线局域网媒体访问(MAC)和物理(PHY)层规范[S]. 2003.

[4] IEEE Standard 802.11i-2004 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 6: Medium Access Control (MAC) Security Enhancements[S]. 2004.

[5] Edney J, Arbaugh W A. Real 802.11 Security: Wi-Fi Protected Access and 802.11i[M]. USA: Addison-Wesley, 2003-07.

[6] 曹秀英, 耿　嘉, 沈　平, 等. 无线局域网安全系统[M]. 北京: 电子工业出版社, 2004.

[7] 西安西电捷通无线网络通信有限公司. WAPI 安全标准技术白皮书[Z]. (2006-09-02). http://www.iwncomm.com.