第34卷 第22期 计 算 机 工 程 2008年11月
Vol.34 No.22 Computer Engineering November 2008
·网络与通信· 文章编号：1000—3428(2008)22—0115—03 文献标识码：A 中图分类号：TN915.04

集中式 WLAN 体系结构通信协议

向 望[1,2]，王志伟[1]，高传善[1]
(1. 复旦大学计算机科学与工程系，上海 200433；2. 复旦大学信息化办公室，上海 200433)

摘 要：针对传统 WLAN 结构在大规模组网时存在的问题，对集中式 WLAN 体系结构进行分析，研究其通信协议部分。该文介绍了 LWAPP, SLAPP, CTP 和 WiCoP 4 种协议的特性，对 IETF 的 CAPWAP 协议进行分析，讨论了系统框架、工作原理、报文结构及安全特性。
关键词：集中式 WLAN 体系结构；CAPWAP 协议；接入控制器；无线接入点

Communication Protocol of Centralized WLAN Architecture

XIANG Wang[1,2], WANG Zhi-wei[1], GAO Chuan-shan[1]
(1. Dept. of Computer Science and Engineering, Fudan University, Shanghai 200433; 2. Informatization Office, Fudan University, Shanghai 200433)

【Abstract】 Aiming at the problems of large-scale WLAN which using traditional architecture, this paper analyses the centralized WLAN architecture, and researches on the communication protocol. It introduces four protocols: LWAPP, SLAPP, CTP, WiCoP, then discusses the architecture, implementation mechanism, packet format and security of IETF's CAPWAP protocol.
【Key words】 centralized WLAN architecture; CAPWAP protocol; access controller; wireless access point

1 概述

自 1997 年IEEE 802.11 标准提出以来，无线局域网(WLAN)接入速度从最初的 1 Mb/s发展到如今的 54 Mb/s，IEEE 802.11a/b/g标准的相继提出极大地推动了WLAN的扩张。WLAN已经不仅仅是有线网络的补充，而是逐渐往大规模部署和独立组网的方向发展，甚至在一些地方取代了有线网络。传统的WLAN体系结构已无法满足大规模组网需求[1]，因此，IETF成立了CAPWAP(Control And Provisioning of Wireless Access Points)工作组，研究大规模WLAN的解决方案。CAPWAP工作组对目前主流的WLAN解决方案进行研究后，把WLAN体系结构分成 3 种：自治式，集中式，分布式网状网[2]。

传统的 WLAN 体系结构为自治式，把 802.11 标准定义的所有功能都在同一 AP(Access Point)里实现，需要对全网每一个 AP 进行配置、管理、监视及控制，大规模 WLAN 由成百上千个 AP 组成，网管的负担非常大；无线资源管理方面，为达到更好的性能，需要在全网进行动态协调，由于 AP 之间相对独立，要达成这一点非常困难；安全性方面，由于覆盖需求，AP 通常安装在不安全的地方，在 AP 被盗后，静态保存在 AP 中的配置信息成为泄密渠道。同时，如何防止非法 AP 接入也对自治式体系结构的安全性提出挑战。

为了解决自治式体系结构存在的问题，集中式 WLAN 体系结构被提出，并逐渐成为最近的研究热点。CAPWAP 工作组正致力于制定出一套基于集中式 WLAN 体系结构的标准，以解决大规模 WLAN 中的网管、安全、资源管理和互操作性等问题。

2 集中式 WLAN 体系结构

2.1 体系结构

从图 1 可以看出，相比自治式结构，集中式 WLAN 体系结构增加了接入控制器(AC)这个要素，AC 可以看作是一组逻辑设备，实现了全网的管理、监控、动态配置、AAA 等功能。无线接入点(WTP)与 IEEE 802.11 标准中定义的 AP 有所不同，AP 实现了 802.11 的所有功能，而 WTP 只需实现部分功能，因此可把 WTP 看作轻量级 AP。AC 与 WTP 之间有 3 种连接方式：直接连接，2 层交换连接和 3 层路由连接。其中，3 层路由连接使 WTP 可通过 IP 网络连接 AC，不仅使 WTP 的部署更加灵活，且解决了无线终端(STA)的无缝 3 层漫游问题，是被广泛采用的连接方式。

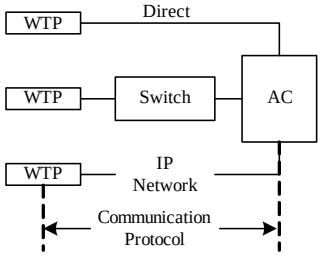

图 1 集中式 WLAN 体系结构

如何在 AC 和 WTP 上实现各种功能，如何实现 AC 对 WTP 的管理，及如何保证通信安全，是集中式 WLAN 体系结构的研究重点。

2.2 功能实现机制

除了 IEEE 802.11 定义的功能以外，CAPWAP 工作组定义了几类 CAPWAP 功能：射频管理，射频配置，WTP 配置，WTP 固件装载，STA 信息数据库和 WTP/AC 相互认证。在集中式 WLAN 体系结构中，大部分 CAPWAP 功能在 AC 上实现，802.11 的物理层(PHY)功能在 WTP 上实现，而 MAC 功能有 3 种实现机制：本地 MAC，分离 MAC，远程 MAC。

本地 MAC 是把 MAC 与 PHY 功能同在 WTP 实现；分离 MAC 是把 MAC 功能中非实时部分置于 AC，实时部分置于

作者简介：向 望(1981－)，男，硕士研究生，主研方向：计算机网络，信息工程；王志伟，硕士研究生；高传善，教授、博士生导师
收稿日期：2008-01-10 **E-mail：**cgao@fudan.edu.cn

WTP；而远程 MAC 是把 MAC 功能在 AC 实现，与 PHY 功能完全分开。例如，STA 与 WTP 的关联(association)功能，在本地 MAC 机制里是在 WTP 上实现，而分离 MAC 机制里是在 AC 上实现。

2.3 通信协议

在集中式WLAN体系结构中，需要有一套机制来实现AC对WTP的管理，于是多种通信协议被提出[3]。

(1)轻量接入点协议[4](Light Weight Access Point Protocol, LWAPP)，描述了全面的AC发现、安全和系统管理方法，支持本地MAC和分离MAC机制。LWAPP提供了一套基于证书和共享密钥的安全机制，在AC和WTP之间建立数据和控制信道，两者可通过 2 层或 3 层连接，2 层连接使用以太网帧传输，3 层连接使用UDP传输LWAPP报文。通过抓包分析结果可看出，LWAPP封装的数据报文和控制报文分别使用UDP 12222 和 12223 端口，首部带有分组标志位，实现方式类似于IP分组。

(2)安全轻量接入点协议(Secure Light Access Point Protocol, SLAPP)，支持桥接和隧道 2 种本地 MAC 机制，支持 WTP 端加解密和 AC 端加解密 2 种分离 MAC 机制，支持直连、2 层和 3 层 3 种连接方式。使用成熟的技术标准来建立通信隧道，数据信道使用 GRE 技术，控制信道则使用安全的 DTLS 技术。

(3)CAPWAP 隧道协议(CAPWAP Tunneling Protocol, CTP)[5]，利用扩展的SNMP对WTP进行配置和管理，虽然实现了AP与WTP互相认证及一套基于AES-CCM的加密规则，但是并不完善。CTP的控制消息着重于STA连接状态、WTP配置和状态几方面。

(4)无线局域网控制协议(Wireless LAN Control Protocol, WiCoP)，定义了包括 WTP-AC 性能协商功能在内的 AC 发现机制，定义了 QoS 参数。协议建议使用 IPsec 和 EAP 安全标准，却并未详细说明实现方法。

LWAPP 具有完整的协议框架，定义了详细的报文结构及多方面的控制消息元素，但全新制定的安全机制还需实践验证，而 SLAPP 使用业界认可的 DTLS 技术是其亮点。相对前两者而言，CTP 和 WiCoP 实现了集中式 WLAN 体系结构的基本要求，但考虑不够全面，特别是安全性方面有所欠缺。CAPWAP 工作组对以上 4 种通信协议进行评测后，最终采用 LWAPP 协议作为基础进行扩展，使用 DTLS 安全技术，加入其他 3 种协议的有用特性，制定了 CAPWAP 协议。

3 CAPWAP 协议

3.1 协议简介

CAPWAP 协议基于集中式 WLAN 体系结构，AC 和 WTP 之间通过 IP 网络连接，旨在达到以下目标：

(1)通过 AC 对 WLAN 系统集中执行强制策略和认证，对系统中的 WTP 进行统一配置，把用户流量集中进行桥接、转发和加密，以增强大规模 WLAN 的可管理性，提高 WLAN 的性能。

(2)使 WTP 不再处理高层协议，只执行与无线访问和控制相关且时间关联性强的功能，以有效利用 WTP 的硬件资源。

(3)提供一类封装和传输机制，使 CAPWAP 协议能够被应用到多种类型的无线接入点上。

协议支持本地 MAC 和分离 MAC 2 种模式。图 2 说明在本地 MAC 模式下，WTP 对无线帧进行处理，然后封装成 IEEE 802.3 帧转发到 AC；而在分离 MAC 模式下，无线帧直接被 WTP 封装后转发到 AC。

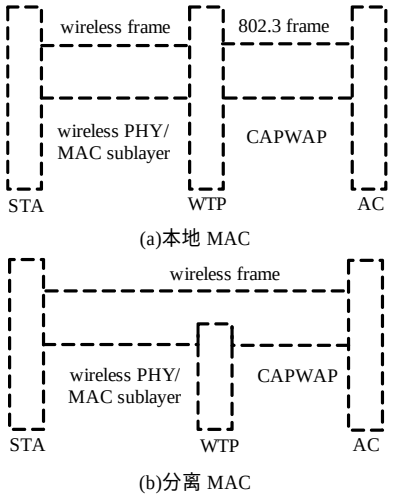

图 2 CAPWAP 协议系统框架

3.2 工作原理

WTP 被连接到网络时即进入发现 AC 的过程。WTP 使用广播、组播或单播方式发送“发现请求”，当使用单播方式时，需首先通过 DHCP 或 DNS 获得 AC 的 IP 地址列表。收到请求的 AC 返回“发送应答”给 WTP，WTP 在应答的 AC 中，选择一个建立 DTLS 连接。

DTLS 连接建立成功后，WTP 发送“加入请求”，AC 回复“加入应答”确认 WTP 加入该 AC 的管理范围。若 WTP 的固件版本过期，则进入升级固件过程，WTP 从 AC 下载最新版本的固件，升级成功以后重启，重新进入发现过程；若 WTP 固件为最新版本，则从 AC 下载配置参数，随后进入运行阶段。图 3 为工作原理示意图。

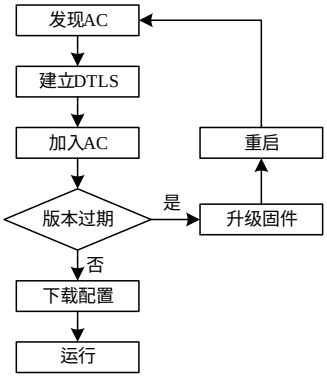

图 3 CAPWAP 工作原理示意图

在运行状态中，AC 通过控制报文动态更改 WTP 配置，获取 WTP 运行状态、STA 信息、射频信息等，由于所有数据都集中在 AC 进行处理，因此可以很容易实施全网级的 QoS、动态射频管理等策略。

3.3 报文结构

CAPWAP 协议规定 AC 和 WTP 的通信分为控制报文和数据报文，控制报文只在 AC 和 WTP 之间传输，实现配置、管理、监控等功能，数据报文则是将被转发的用户数据帧。2 种报文通过不同的 UDP 端口进行传输，控制报文中除“发现请求/应答”是明文传输以外，其他的强制使用 DTLS 保护，而数据报文可选择是否使用 DTLS。

报文结构如图 4 所示。

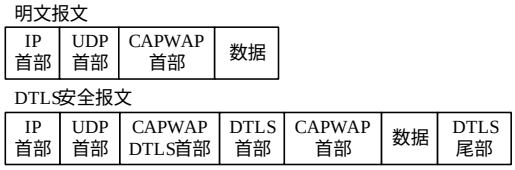

图 4　CAPWAP 报文

3.3.1　预判码

2 种 CAPWAP 首部的前 8 位为预判码，用于快速判断此报文是否经过 DTLS 加密。前 4 位指明 CAPWAP 版本，目前的版本号为 0；后 4 位值为 1 时是 CAPWAP DTLS 首部，值为 0 时是 CAPWAP 首部。

3.3.2　CAPWAP DTLS 首部

标识此报文经过 DTLS 加密。长度为 32 位，包括 8 位预判码和 24 位预留码。

3.3.3　CAPWAP 首部

CAPWAP 协议的所有报文都包含 CAPWAP 首部，在控制信道收到则是控制报文，在数据信道收到则是数据报文，图 5 描述了 CAPWAP 首部的结构。

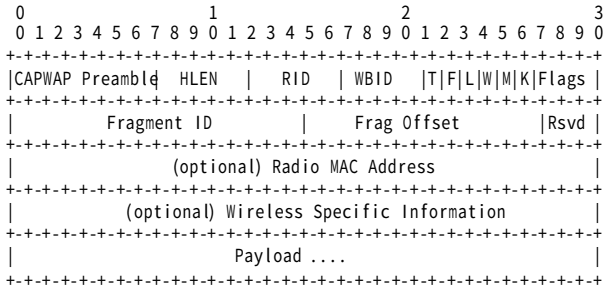

图 5　CAPWAP 首部

报文各部分组成如下：

(1)CAPWAP Preamble：8 位预判码，参见 3.3.1 节。

(2)HLEN：5 位首部长度，指明 CAPWAP 首部的长度。

(3)RID：5 位射频标识符，指明此报文的来源射频。

(4)WBID：5 位无线帧标识符，指明无线帧类型，有 IEEE 802.11, IEEE802.16 和 EPCGlobal 3 种。

(5)T：1 位数据帧标识符，值为 1 时数据帧是由 WBID 指明的类型，值为 0 时是 IEEE802.3 数据帧。

(6)F：1 位分组标志，值为 1 时此报文是一个 CAPWAP 报文分组，需要和其他分组重组成完成的报文。

(7)L：1 位分组结束标志，值为 1 时此报文是最后一个分组。

(8)W：1 位选项标志，值为 1 时存在 Wireless Specific Information 选项。

(9)M：1 位选项标志，值为 1 时存在 Radio MAC Address 选项。

(10)K：1 位存活标志，指明此报文用于保持连接存活，不能携带用户数据。

(11)Flags：3 位预留标志。

(12)Fragment ID：16 位分组标识符，识别不同的报文分组，ID 相同的分组属于同一个 CAPWAP 报文。

(13)Fragment Offset：13 位分组位移，各分组在该 CAPWAP 报文中的位置。

(14)Reserved：3 位预留码。

(15)Radio MAC Address：32 位射频 MAC 地址，不足 32 位以全 0 填充。指明报文来源射频的 MAC 地址。

(16)Wireless Specific Information：32 位特殊无线信息，不足 32 位以全 0 填充。包含特殊信息，如与 IEEE 802.11, IEEE802.16 和 EPCGlobal 的关联等。

(17)Payload：数据报文是用户数据，控制报文则是控制消息，详细的控制消息定义参见文献[1]。

3.4　安全特性

CAPWAP 协议使用 DTLS 技术进行加密和认证，保证了 AC 和 WTP 之间的传输层安全，但“发现请求”报文是明文发送，有可能遭遇伪装攻击。CAPWAP 强调 AC 在收到“发现请求”后不要立即终止与该 WTP 的原有会话，而是新建一条 DTLS 连接，直到成功以后再移除旧连接。

CAPWAP 定义了 AC 和 WTP 互相认证的机制，可防止非法 AC 和 WTP 接入 WLAN 系统。同时，AC 能监控全网络的无线射频资源，拥有足够的信息对系统外的 WTP 进行探测和定位。

WTP 的配置参数是在成功加入 AC 以后再下载到内存，WTP 本身几乎是零配置，即使被盗也不会泄漏 WLAN 系统信息。

4　结束语

集中式 WLAN 体系结构能很好地解决传统 WLAN 体系结构存在的问题，但多样化的通信协议仍然给大规模组网带来不便。CAPWAP 协议在部分地方还存在争议，如报文在 IPv6 网络中传输是使用 UDP-Lite 还是 UDP 等，CAPWAP 工作组正在进行最后的讨论和修改。待协议正式发布，有望结束目前不同厂商 AC 和 WTP 无法互通的局面，使建设大规模 WLAN 系统更加灵活，不再局限于使用统一型号的 WLAN 设备。

参考文献

[1] Hara B O, Calhoun P, Kempf J. Configuration and Provisioning for Wireless Access Points(CAPWAP) Problem Statement[EB/OL]. (2005-02-13). http://www.ietf.org/rfc/rfc3990.txt.

[2] Yang L, Zerfos P, Sadot E. Architecture Taxonomy for Control and Provisioning of Wireless Access Points(CAPWAP)[EB/OL]. (2005-06-07). http://www.ietf.org/rfc/rfc4118.txt.

[3] Calhoun P, Montemurro M, Stanley D. CAPWAP Protocol Specification[EB/OL]. (2007-06-11). http://tools.ietf.org/id/draft-ietf-capwap- protocol-specification-07.txt.

[4] Loher D, Nelson D, Volinsky O, et al. Evaluation of Candidate Control and Provisioning of Wireless Access Points(CAPWAP) Protocols[EB/OL]. (2006-06-21). http://www.ietf.org/rfc/rfc4565.txt.

[5] Calhoun P, Hara B O, Suri R, et al. Light Weight Access Point Protocol[EB/OL]. (2007-03-20). http://www.ietf.org/internet-drafts/draft-ohara-capwap-lwapp-04.txt.