网络图中的平行工作等。

（3）外部依赖关系：指关系和影响到活动的时间安排及效率的，任务具体活动与相关的非任务活动之间的关系。如：相关的硬件是否到货，人员是否能及时到场，场地方要求某些时段不允许我方工作等。直接影响双代号网络图中具体工作的工作时长；以及由于人员、机器限制形成的先行、后续关系等。

在应急基站的开通活动中，强制性的依赖关系包括：A->B；D->E；B->C；B->G；B->H；E->H。可灵活处理的依赖关系包括：B 与 E；F 与 C；F 与 B，H 与 C；G 与 C；D 与 C；D 与 B；E 与 C；在此基础上，更进一步的紧前紧后关系需要结合具体的应急基站确定。

3.3 双代号网络分析

在活动拆解排序的基础上，选择较为常见的（卡车改装应急通信车+大型油机车+光缆的应急基站类型）为对象。确定双代号网络逻辑关系并预估各活动耗时情况。

（1）双代号网络及相关参数

具体情况如表 1：

表 1　双代号网络及相关参数

工作	A	B	C	D	E	F	G	H	I
紧前工作	--	A	B	A	B	B	E，F，D	G，C	H
时间（小时）	3	2	1	1	3	0.5	1	1	0.5

则可以得到对应的双代号网络关系及各个工作的六时间参数情况如图 1。

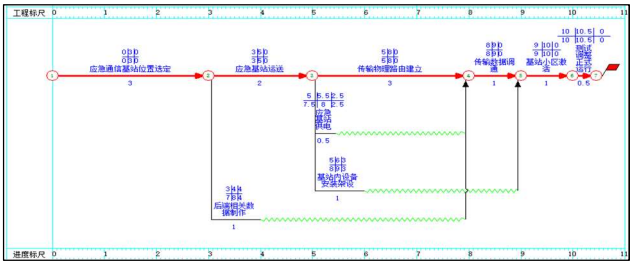

图 1　应急通信基站双代号网络图

该项目的关键路径为应急通信基站位置选定->应急基站运送->传输物理路由建立->传输数据调通->基站小区激活->测试调整投入运行。关键路径上的每一个工作都是关键工作。关键工作的延误都会造成总工期的延长，也是投入资源缩短工期的主要着力点。

总时差>0 的工作包括：应急基站供电（总时差 2.5），后端相关数据制作（总时差 4），基站内设备安装架设（总时差 3）。在这个网络图中，由于其紧后工作恰好都是关键工作，所以总时差=自由时差。这些工作提前完成和在总时差范围内的延误和对总工期不会产生变化。

（2）双代号网络分析及优化

在网络图绘制以后，结合关键线路处理和实际情况可以展开深度和相对精确的调整优化。总结双代号网络技术可以在时效角度可以从时间，时间资源，时间成本三个方面对应急基站情况予以分析。

第一，对时间进行优化。通过双代号网络图可以精细比对不同应急基站开通形式的时效结构，通过各个具体活动时间定量评估总工期，进而结合实际场景进行方案优选。在方案选定实施时，可以根据双代号网络技术对应急基站开通情况实行进度检查，精准判断相应的活动进度现状是否会导致总工期超前或者滞后。

第二，时间-资源优化。在实际工作中，各个具体活动的完成需要投入人力，设备，动力等资源。当资源有限，或者多个应急车同一个队伍开通出现人力，设备资源复用的情况时，可以应用双代号网络技术结合具体工作的总时差，以应急基站开通时效为目标对多个工作资源安排组合调整调整优化。在需要增加进度时，可以通过双代号网络技术确定关键工作和实际资源限制情况，清晰资源投入方向。

第三，时间-成本优化。每个活动的完成需要投入资源也必然会带来成本，应用双代号网络技术可以结合各个具体活动的时间参数和各个活动成本投入结构，在不影响工期情况下，通过时间参数时差的应用优化成本结构。在需要压缩总工期的情况，对投入成本最低的关键活动压缩。实现压缩高成本活动同样的效果，同时避免压缩具有总时差的活动导致投入资源对工期提前没有作用的情况。对时间-成本活动实现精细优化。

4　应急基站时效的控制

时效的控制一方面指在对完成任务具体活动进行深入演练和人员技能熟练程度规范和提高的基础上，通过应急基站开通完成时间的目标的进度检查，对超前，滞后以及意外情况或者新增工作对完成时间的影响判断及调整措施。另一方面则指在达到时间目标的前提下，对投入的资源，消耗的成本以及必要调整变更的资源和成本进行精细控制。

应用双代号网络技术，可以应急基站的开通进展总工期为目标在过程中进行的进度检查；在日常演练中可以对关键路径的工作重点提升；在遇到滞后需要调整时可以比对各个关键工作所消耗的资源和风险，可以辅助科学直观选择低风险低消耗的工作投入资源却达到同样效果；对拥有总时差的工作可以充分利用时间参数适当滞后或者分散资源等。

由上可见，双代号网络技术可以为应急基站时效控制的能力的整体提升提供了深入细致和系统全面的科学手段。

5　结束语

目前应急基站能力提升主要在活动完成的演练，对时效控制方面由于缺乏系统工具和理论一直较为粗放。本文从时效的角度对应急基站的开通和属性进行探讨。首先明晰了应急基站的开通过程，并根据任务固有的特性，拆解定义为不同的活动。在此基础上引入了双代号网络技术进行时效分析。通过双代号网络技术时间参数，关键线路，关键路径的确定，可以实现应急基站开通时间，时间-成本，时间-资源三个方面的系统分析优化，精细管控。时间分析后，应急基站能力提升与双代号网络技术系统适配度高，具有较大的推广意义。

参考文献：

[1]柳纯录.系统集成项目管理工程师教程[M].清华大学出版社，2009.

[2]陈思茹.通信工程项目中的双代号网络优化技术研究[J].电子世界，2016（07）：72-73.

校园无线局域网的安全保障策略研究

◆何儒锋

（河源市卫生学校　广东　517000）

摘要：近年来，随着无线局域网技术及相应产品的渐趋成熟，无线局域网在各行各业的应用越来越普及，各个学校的也基本实现了“有线+无线”模式的校园网络全覆盖，但由于无线局域网的开放性却使这种模式的校园网面临了不少新的安全挑战，对此本文将从分析校园无线局域网的安全隐患入手，探讨如何实施安全策略来保障校园网的安全。

关键词：数字化校园；无线局域网；安全隐患；安全保障策略

1　引言

目前，我们早已步入了信息化社会，进入了互联网时代，越来越多的学校也建设了数字化校园，校园网已成为是在校师生获取学校资源和信息的主要途径，特别是无线局域网技术及无线客户端的普及，

让师生在校内可以随时随地访问校园网资源及获取互联网资源，为学校的教学、管理和科研等工作提供了极大的帮助及便利。

但是，由于校园环境的开放特点，常常会有很多访客甚至是一些无关人员进入到校园网络覆盖范围内，如果这些未授权人员可以任意的通过无线网络的方式接入校园网，必然会对校园网络的完全构成威胁，在日常生活中也常会出现由于管理不当，安全意识薄弱等原因导致的信息泄露等事件。这就需要我们对校园网内的无线局域网存在的安全隐患有清晰的了解，并针对性实施无线局域网的安全保障策略来保障我们的校园网络的安全。

2　无线局域网的安全隐患

无线局域网技术是以无线广播信号为基础的网络通信技术，这种技术天然具有开放性的特点，使用户能非常方便地接入网络，但这种便捷性同时也给校园网络的安全保障带来了不小的安全挑战。与有线网络相比，无线局域网主要面临以下安全威胁：

首先，由于无线网络信号天然具有的开放性，使无线用户客户端不用与无线局域网发生实际上的物理连接，未授权的非法用户只需要使用与无线局域网具有相同的技术标准的客户端，即可轻易地截获局域网内的无线网络信号，使得非法入侵者可以更简单地伪装成局域网内的合法用户。

其次，由于无线局域网通信技术是基于电磁波的广播信号，这就使无线局域网内无法像传统有线网络那样可以通过物理隔离手段来保障整个网络的安全，无法阻止未授权的非法用户对无线局域网的攻击及无线设备之间通信数据窃听。

3　无线局域网的安全策略

在无线局域网中，主要是通过用户身份认证技术和通信数据加密技术等手段来保障数据安全。为应对无线局域网中通信窃听及信号伪装等安全隐患，本文主要从无线局域网的接入策略、接入技术、传输安全及网络分段四方面来探讨校园无线局域网的安全保障。

3.1 接入策略

3.1.1 不同用户群的接入策略

为了便于管理，首先需要对校园局域网的用户根据不同的特性划分为不同的用户群，并赋予不同的校园网络资源访问权限。本文将用户群分为：在校师生，中长期访客，临时访客三个用户群，对不同用户群采用不一样的接入策略。

（1）对于在校师生用户群，可以设立一组长期的用户账号，并将接入校园无线局域网的连接认证与校内其他已有的认证系统相统一，这样可以在不增加新的账号和密码的情况下，实现校园“一卡通”，“一号通”。

（2）对于中长期访客，如来校培训人员，可以为这类用户增加单独的账号群，并由校园网络管理人员根据访客的实际情况授权访问特定校园网络资源。

（3）对于短期来访的客人，如到学校参加会议的与会人员，则可以设立一组临时账号来让这类用户访问特定的网络服务。

3.1.2 不同地点的接入策略

在实施针对不同用户群设置不同接入策略的同时，还可以根据校内的不同地点、不同场景采用不同的校园网接入策略。这种接入策略主要是通过配置管理不同网络节点的交换机来将校园网按区域和场景分隔成不同的若干个更小的局域网来实现，主要可以分为以下几个不同区域的接入配置策略：

（1）教学楼外、校园广场等室外公共区域。由于无线信号覆盖范围广，且在这类区域活动的人员较复杂，流动性强，导致学校无法对校园网络进行有效管理。为了保障校园网络的信息安全，对于在这类区域接入校园无线局域网的无线客户端，应当采用更加严格的通信加密技术及用户认证方式。如采用 Web portal 认证技术和 802.1X 认证技术并存措施，这样既能保证在校师生和来访用户都可以方便地接入校园无线局域网，同时又能降低网络被攻击的风险，保障校园网络的安全。

（2）会议室及报告厅等临时使用的室内区域。由于这类区域只在有会议或报告的时候才开放，对网络的使用需求是临时性的，用户需要的是能够更方便、快捷的接入校园网络，所以在这类区域的无线客户端设置需要尽量简单，最好是免设置，使与会人员可以快速接入网络；因此，在这类场景中应采取开放式认证方式和广播网络信号的配置策略，以简化这类用户的校园网络接入过程。在室内区域由于墙壁对无线信号具有一定的屏蔽作用，且只在会议期间使用网络，加上用户身份容易确定，所以校园网络管理员可以通过控制网络信号的开关的方式来控制这类区域网络的使用，因此，在这类区域的网络使用不会有太大的安全问题。

3.2 接入技术

除了从校园网络管理方面入手根据不同用户群及不同接入地点采用不同接入策略外，还可以从接入技术方面考虑，通过使用以下技术来保障校园无线局域网的信息安全：

3.2.1 采用 MAC 地址过滤

由于无线网卡的物理地址即 MAC，具有唯一性，因此校园网的管理员可以在无线访问接入点（AP）中设置一份无线客户端的 MAC 白名单，这个技术可以将不在 MAC 白名单内的无线客户端过滤掉，从而达到限制未授权非法设备接入校园网络的目的。但该方法只能让提前录入 AP 白名单的无线客户端接入校园网络，对大量的中短期访客不适用，且无法识别通过篡改 MAC 地址伪装成合法用户的未授权非法用户访问校园网络。

3.2.2 采用 802.1X 协议认证技术

802.1X 协议认证技术是一种无线网络认证方案，在实施了该认证技术方案的无线局域网中，无线用户端安装 802.1X 协议客户端软件，无线访问接入点（AP）中内嵌 802.1X 协议认证，并作为设备访问校园网络的第一道安全门。在无线客户端认证通过前，该协议只允许基于认证协议的认证数据通过 AP，只有认证通过后才能让正常的网络数据通过 AP 的端口，如果认证失败，则禁止该无线客户端访问校园网资源。

3.2.3 采用 Web portal 认证方式

Web portal 是一种更加简便的无线网络用户认证方案，该方案适合部署在对网络安全要求不是特别高但有大量临时无线访问需求的地方。该认证方式最大的特点是免客户端软件，只需要在浏览器中用自助服务的方式通过认证即可访问网络。该方式使用 HTTPS 方式也能对用户认证数据通信提供一定的安全保护，使校园网在保证了安全性的同时又极大地提高了便利性。

3.3 传输安全

无线局域网作为一种以电磁波作为载体的通信技术，使无线网络信号具有开放性，因此在无线网络信号的覆盖区域内，任何一个遵循特定标准的无线客户端都可以接收到该网络的信号，这样就可能导致无线局域网内用户的通信数据被其他未授权的非法客户端截获。这也就使得使用无线网络的用户相对于使用有线网络的用户更容易被非法用户窃听数据或干扰信息的传输。

为解决以上数据传输的安全问题，从传输技术角度入手，还可以采取以下方式来保障安全：

3.3.1 关闭服务集标识 SSID 广播

服务集标识，即：SSID（Service Set Identifier），该技术可以将一个无线局域网分为若干子网络，每个子网络用唯一 SSID 进行标识。在一些开放区域，为了更好地提供网络服务，都会将无线接入点的 SSID 设置为广播状态，这样就可以使无线信号覆盖范围内的所有无线客户端都可以搜索到可用 AP 的 SSID，从而可以很方便地接入网络。但这种对外广播 SSID 的方式同时也存在一定的安全隐患，即未授权的非法用户也可以通过搜索到的 SSID 接入无线网络，因此可以采取在特定区域关闭 AP 的 SSID 广播的方式来管理，这样无线客户端就必须在指定区域设置正确的 SSID 才能与对应的 AP 进行通信，从而减少了非法用户的接入。

此外还可以采用无线信号加密技术来保障无线通信数据的安全，这样即使无线通信数据被窃听也可以保证通信内容无法被破解、读取，目前主要有 WEP，WAP 两种加密技术可以为无线信号提供安全且稳定的加密。

3.3.2 采用 WEP 技术加密通信数据

WEP 是 Wired Equivalent Privacy 的简称，有线等效保密（WEP）协议是 IEEE802.11b 标准规定一种可选的加密方案，该方案可以对设备间无线传输的数据进行加密，使无线局域网具有与有线网络相同级别的安全保护，用来阻止未授权的非法用户窃听 AP 与无线客户端之间的传输内容或入侵无线局域网。

3.3.3 采用 WPA 技术加密通信数据

WPA 全名为 Wi-Fi Protected Access，有 WPA、WPA2 和 WPA3 三个标准，是一种保护无线电脑网络（Wi-Fi）安全的系统，WPA 采用 802.1x 协议和 TKIP 来实现对无线局域网的访问控制、密钥管理与数据加密，TKIP 是一种基于 RC4 加密算法，对现有的 WEP 进行了改进，为无线通信传输的数据提供了更高等级的安全保护。

3.4 把网络分段

从阻止未授权非法用户访问校园网络资源的角度来管理，还可以

用虚拟局域网（VLAN）技术将具有不同访问权限的用户群隔离开来，可用具备 VLAN 功能的交换机来实现这一目的。VLAN 技术是将在通过同一物理设备访问物理网络的用户，划分为多个虚拟的逻辑网络，从而将不同的用户群分隔开来，并赋予不同的校园网络资源访问权限。如同样在广场等开放区域，所有用户都接入相同的 AP，但是可以利用有 VLAN 功能的交换机划分多个用户群；将临时访问的用户划分为一个用户群，这类用户只需要进行简单的身份认证就能接入校园网，但是通过这个 VLAN 访问的用户只能进行简单的开放资源的查询，浏览新闻等操作。而对于在校师生这类长期的固定用户群又划分为一个用户群，这类用户如果想访问校园网络则需要进行更严格的身份认证，认证通过后除了有基本的网络访问权限，还能访问到更多更核心的校内教学资源等。

4 结语

当然，跟有线局域网比起来，无线局域网通信技术仍然还有不少问题与挑战，如无线局域网的传输速度还有很大的局限性，无线信号容易被干扰对通信环境的要求较高，同时还有不少的通信数据安全隐患等。但随着无线通信技术的成熟及组网成本的下降，无线局域网将会在校园网络及各行各业的建设中发挥越来越重要的作用。

参考文献：

[1]吕宏强.浅谈无线网络安全防护[J].网络安全和信息化，2021（6）：37-39.

[2]刘明辉.校园无线网络安全管理风险和防范技术研究[J].长春大学学报（自然科学版），2010，20（1）：68-70.

[3]刘健.高校校园网络存在的安全隐患及防范技术探讨[J].网络安全技术与应用，2015（7）：29-30.

[4]姜凯文.高校无线局域网用户认证控制及管理机制[J].电脑迷，2018（7）：101-102.

[5]赵娟.无线局域网 802.11x 技术[J].网络安全技术与应用，2010（8）：23-25.