城市轨道交通车地无线通信安全性分析

陈　帆，金斌斌*，许平超

（中兴（温州）轨道通讯技术有限公司，浙江 温州 325000）

摘　要　车地无线通信作为城市轨道交通车地调度指挥系统的核心技术之一，是保证列车运行安全和提高运输效率的重要保障。本文分析了城市轨道交通车地无线通信技术中存在的安全隐患问题，指出了车地无线通信网络安全性提升过程中需要解决的关键技术问题，提出了基于WPA-PSK/4 PSK与FLEX加密体制相结合的车地无线通信加密方案，并给出了该方案在城市轨道交通车地无线通信网络中应用时的具体实现方案。

关键词　城市轨道交通；车地无线通信；安全性

中图分类号：U12　　**文献标识码**：A　　**文章编号**：1007-0745(2023)05-0019-03

车地无线通信系统的主要组成部分是车载计算机、车载调度台、固定站及无线网络等。车地无线通信系统的关键技术是基于IEEE802.11无线局域网（WLAN）技术的车地无线通信技术，该系统主要用于保证城市轨道交通车地调度指挥，是城市轨道交通运行的重要保障。当前，在城市轨道交通领域广泛应用的主要车地无线通信技术包括WLAN（基于802.11标准）、WiMax（基于802.11b标准）和WPA-PSK/4 PSK（基于IEEE802.11g标准）等，这些车地无线通信技术中普遍存在着安全隐患问题，对于城市轨道交通车地无线通信安全管理、安全防护等工作带来了一定的影响。

1 车地无线通信技术面临的安全隐患

城市轨道交通无线通信网络不仅承载了大量的实时数据和控制命令，而且还承载着大量的列车控制数据和服务信息，因此车地无线通信网络面临着巨大的安全隐患。具体来讲，车地无线通信网络可能面临以下几种安全隐患。

1.1 被窃听者截获通信信息后进行窃取

若窃听者使用有效的窃听者工具进行窃听，那么其会截获一系列合法用户发送的数据包，然后根据窃听者的截获数据进行分析和破解，从而获取车载系统、ATS/ATO系统、CBTC系统和无线基站等设备发送和接收到的各类数据。

1.2 被恶意篡改或伪造

攻击者可以利用相关设备对车载网络进行篡改或伪造，使车载网络不能正常运行或通信中断。比如，恶意篡改车载网络中的相关协议、配置文件等；恶意修改车载系统中的相关配置参数、消息收发状态等。

1.3 被控制终端伪造、篡改或者窃听

车辆控制终端可以通过网络直接或间接控制车载系统等设备；通过修改车载系统中的相关协议、配置文件等达到控制车辆的目的。

2 车地无线通信网络安全增强需求

在城市轨道交通车地无线通信网络中，各系统设备之间的通信数据需要经过车地无线通信网络进行传输，因此车地无线通信网络对信息传输的安全性要求非常高，主要表现在：

首先，必须保证在传输过程中不被非法截取。车地无线通信网络是一个开放性的网络，且各系统设备之间的数据交互频繁，信息数据被截获和篡改的可能性非常大。因此，需要在无线通信网络中增加对传输数据的加密措施，使其无法被截获。

其次，数据完整性保证。由于车地无线通信网络中存在大量不同设备和用户等不同身份的安全实体，如果能够对这些信息进行有效的加密并在传输过程中实时校验，则可保证信息传输的完整性。

最后，设备身份验证与通信会话密钥协商。车地无线通信网络中存在大量不同身份的安全实体，如用户、终端、列车等。如果没有对这些设备进行有效的身份验证和认证，就无法确保它们之间以及它们与中心服务器之间的会话密钥协商，就无法保证车地无线通信网络系统能够正确地将数据传输给正确的用户。

综上所述，车地无线通信网络必须要建立一种安全有效的数据传输机制来保护车载设备、乘客和列车

*本文通讯作者，E-mail：1169621818@qq.com。

司机之间直接交互所形成的数据信息安全。

2.1 增强需求

现阶段，在城市轨道交通中实现安全的措施主要采用无线通信系统，这样可以有效地降低成本，并且由于其在城市中使用方便、操作简单和建设周期短，因此可以较好地解决轨道交通线路覆盖范围内的信号覆盖问题。但是无线通信系统也存在一定的缺点：首先，无线通信系统需要消耗大量的电能，这样就会造成巨大的经济负担；其次，无线通信系统在网络传输过程中容易受到黑客攻击，造成数据信息泄露。

车地无线通信网络中基于安全协议的安全性增强需求主要包括：（1）在车载设备和地面设备之间进行安全认证；（2）采用非对称加密算法对信息进行加密；（3）使用安全实体对信息进行完整性校验；（4）数据传输过程中采用明文传输或加密传输。此外，还可以使用设备身份验证与会话密钥协商来保护通信过程中的安全，从而保证车地无线通信网络系统安全运行[1]。

2.2 相关技术分析

无线基站的安全性主要体现在数据传输过程中的机密性和完整性方面。为了解决车地无线通信网络中数据传输过程中的安全问题，可以采用密钥管理。从安全角度出发，使用合适的密钥管理算法是最简单、最有效的方法。虽然目前针对密钥管理已有多种算法，但在城市轨道交通领域，仍没有一种算法是能满足所有情况需要，并且适用于所有业务环境的。目前对于城市轨道交通无线通信网络所使用的密钥管理算法主要包括基于椭圆曲线公钥密码体制（ECDH）、基于非对称椭圆曲线公钥密码体制（AES）以及基于数字签名技术（ECDH、DTS、SET）等。其中，基于非对称椭圆曲线公钥密码体制（AES）是应用最广泛的密钥管理算法，也是目前最安全实用和有效的密钥管理方案。然而，由于这种算法对运算速度和计算资源要求较高，其适用范围也受到限制。而ECDH、ECDH+DTS等算法在密钥生成时使用非对称加密技术，既可满足数据加密要求，又可满足密钥管理需求。

3 安全增强方案

目前，国际上公认的安全标准是ISO/IEC 17901。该标准针对无线通信网络的安全问题，在加密技术、密钥管理以及安全认证等方面进行了全面的研究。其中，以采用基于对称密钥体制、非对称密钥体制以及公钥基础设施等措施为代表，是当前国际上公认的城市轨道交通车地无线通信网络的安全增强方案。

本文提出一种基于WPA-PSK/4 PSK与FLEX加密体制相结合的车地无线通信加密方案。该方案是采用对称密钥体制，加密和解密使用不同密钥进行操作。用户端使用WPA-PSK/4 PSK和FLEX体制进行加密，而用户终端的用户端使用非对称密钥，以实现数据保密性及数据完整性。

3.1 加密体制

车地无线通信系统的加密体制采用了FLEX和WPA-PSK/4 PSK相结合的方式。首先，在用户端选用WPA-PSK/4 PSK进行加密，将数据加密成128 bit的数据块，然后将数据块以密文形式传输给用户终端。用户终端利用密钥对数据进行解密，将得到的加密后的数据再发送给用户端。而在用户端需要传输加密后的信息时，则采用FLEX体制进行加解密处理。FLEX体制是基于RSA算法基础上发展起来的一种对称密钥体制，它最大的特点是密钥生成算法简单、计算成本低，而且便于实现。此外，FLEX体制具有密钥生成快、安全性高、抗毁性强等特点，适合应用于安全等级要求较高的场合。该方案的优点是：在加密过程中仅需一次密钥更新即可完成对数据进行加解密处理；在加密和解密过程中，对用户端不要求必须具备硬件平台，只需要有一台能满足该体制要求的终端设备即可。同时，该方案还具有很强的可扩展性，能够实现动态加解密功能[2]。

3.2 密钥管理

通常，城市轨道交通无线通信网络中，存在大量需要加密和解密的信息，这就需要通过密钥来完成。例如，当列车运行至车站时，地面站点与车辆间需要进行加密通信；当列车到达某一站点时，车辆间需要进行解密通信；当列车驶离某一站点时，需要对所有列车的无线通信信息进行加密。因此，对于城市轨道交通车地无线通信系统来说，在不改变现有结构的前提下实现密钥的生成和分发是非常必要的。

一般来说，城市轨道交通车地无线通信系统中存在大量需要加密和解密的信息，如车门开关、列车车门位置、屏蔽门位置及车站设备信息等。在这些信息中，除了包含有一些常用信息外，还存在着许多特殊信息。如果没有足够安全有效的密钥对这些特殊信息进行加密和解密处理，则会存在一定的安全隐患。因此对于这些特殊信息必须采用非对称密钥进行加密和解密处理。

3.3 安全认证

在城市轨道交通车地无线通信网络中，为保证数据传输的安全性，采用了基于口令与数字证书的双向认证机制。首先，用户端在收到PIS系统下发的密钥后，向PIS系统发起一个“注册”请求，然后以PIS系

统的 ID 作为口令发送给 PIS 系统。此时，PIS 系统根据该用户口令及 PIS 系统的 ID 值验证该用户是否为合法的 PSOA。如果验证通过，则继续进行“注册”操作；否则拒绝注册，并将该用户的口令更新为自己的口令。然后，根据 PIS 系统在收到 Update 请求后将更新后的密钥与相应的 KEY 一起发送给 PIS 系统，并将更新后的 Update 广播给 PSOA，PSOA 通过这个 Update 认证该用户是否为合法用户。如果认证成功，则对该 Update 进行“登录”操作；否则拒绝访问。

4 具体实现方案

车地无线通信系统应符合《城市轨道交通信号系统设备技术条件》（CJT24—2006）的相关要求，同时还应满足城市轨道交通车地调度指挥系统的功能需求。基于 FLEX 加密体制的车地无线通信网络可以保证车地无线通信网络在车地间运行时的安全性，进而实现安全通信 [3]。

为实现该方案，可通过以下步骤进行实现：

1. 建立一个密钥管理中心，并将所有需要进行加密处理的车载设备与其连接，进而实现对车地无线通信系统中无线接入设备的统一管理。

2. 加密处理设备通过公钥认证服务器，与车载设备进行密钥交换，然后通过加密处理设备将加密处理数据发送给车载设备。

3. 车载设备从移动通信机房接收加密处理后的数据并进行解密处理后发送给移动通信机房。在此过程中，对于所发送给移动通信机房的数据进行加密保护，并且在发送数据前进行加密运算操作。对于需要传输至移动通信机房的数据进行解密操作，并对所传输数据进行解密运算操作，之后再将所计算出的结果发送给移动通信机房。在此过程中需要对所计算出的结果进行加解密运算，再将所加解密后的结果发送给移动通信机房。

4. 移动通信机房接收到车载设备发来的解密数据后通过接口将数据转换为 FLEX 密钥对信息进行解密处理，最后将 FLEX 密钥对信息进行加解密运算操作。

5.FLEX 加密体制主要包括：FLEXAd (1) 密钥产生算法和 FLEXAd (2) 密钥管理算法。密钥产生算法是对经过加解密运算得到的密文数据进行再生成新密钥。而密钥管理算法是通过对已知的公钥对密文进行加解密操作，再对所得到的新密钥进行加解密密钥计算。

6. 对加密处理后的信息进行加解密运算后传输至车载设备。当车载设备从移动通信机房接收到加解密后的信息后，通过接口将数据发送至移动通信机房，接收到传输过来的加解密密钥数据后并进行相应操作。

7. 加密处理设备将已经生成加解密密钥和密钥后的信息通过接口发送至移动通信机房中车载设备。该过程与上述过程类似，只不过是将车载设备收到加解密后的信息由移动通信机房发送至移动通信机房中对应设备上 [4]。

8. 从移动通信机房接收到加密处理数据后，再将其通过接口发送至车载设备。此时，在此过程中需要对所接收到的加解密数据进行加解密运算处理。当所接收到车地无线通信系统所使用的 WPA–PSK/4 PSK 体制密钥在采用 FLEX 算法加密后产生新密钥时，则车载设备可以通过接口将新密钥发送至移动通信机房；当所接收到车地无线通信系统所使用 FLEX 算法加密后产生新密钥时，则车载设备可以通过接口将新密钥发送至移动通信机房。

9. 由于该系统对城市轨道交通中所有无线接入设备采用统一管理方式，因此当车辆接入该系统时可以从移动通信机房获取无线接入设备所有密钥信息，再由车载设备通过接口将密钥发送至移动通信机房中对应的车载设备上。同时，该系统还可提供其他具有相同密钥信息的接口，以供其他车辆接入该系统中。

5 结语

车地无线通信是保障城市轨道交通运输安全运行的重要技术，提高车地无线通信网络安全性对于保证城市轨道交通运输安全具有非常重要的意义。本文分析了车地无线通信网络安全问题及主要风险，指出了车地无线通信网络中存在的安全隐患，指出了提升车地无线通信网络安全性应采取的措施。随着科学技术的发展，城市轨道交通必然会朝着更加高效、节能和环保的方向发展。目前，以高铁为代表的新型轨道交通也在向智慧化方向发展。如何确保新技术在城市轨道交通领域应用中的安全，也将是今后研究工作中需要重点考虑的问题。

参考文献：

[1] 蒲豫园 . 城市轨道交通车地无线专用通信系统 5G 技术应用探讨 [J]. 都市快轨交通 ,2022(01):107–113.

[2] 彭显辰 .LTE 在城市轨道交通信号系统车地无线通信中的应用——评《城市轨道交通信号与通信系统》[J]. 现代雷达 ,2021(07):I0014.

[3] 孙全涛 , 崔晓军 , 杜振振 , 等 . 城市轨道交通车辆制动系统的车地无线通信数据传输各环节常见问题分析及解决方法 [J]. 城市轨道交通研究 ,2022(08):25.

[4] 程子宸 , 罗春晓图 . 基于长期演进技术的城市轨道交通车地无线通信技术 [J]. 铁道知识 ,2022(03):50–55.