星闪无线短距通信技术（SparkLink 1.0）安全白皮书 — 网络安全

2022 年 12 月

参编单位

中国标准化研究院、奇安信科技集团股份有限公司、华为技术有限公司、郑州信大捷安信息技术股份有限公司、北京中科晶上科技股份有限公司，北京华瑞赛维通信技术有限公司、长城汽车股份有限公司、成都爱旗科技有限公司、鼎桥通信技术有限公司、吉利汽车中央研究院、上海海思技术有限公司、深圳市摩尔环宇通信技术有限公司、深圳市钛和巴伦技术股份有限公司、深圳市三旺通信股份有限公司、中国电子技术标准化研究院、中国信息通信研究院、紫光展锐（上海）科技有限公司

执笔人

巫小波、王勇、李文昭、王琰、许斯亮、刘为华、肖凌云、谢志利、陈璟、李丛蓉、马骁菲、申俊圣、孙林、万建超、王超、王智玮、夏冀、姚群、曾庆生、张磊、甄斌、郑喆、邹柳

版权声明

前　言

无线短距通信是指在局部区域内，如家庭、办公室、实验室、建筑物内、校园、车间或工厂等，两个无线设备间的通信，这些设备间的距离通常在10~20m以内。无线短距通信使得用户在有限空间内位置移动的同时，始终保持着通信链接。在过去30年间，无线短距通信迅速发展，市场规模巨大。而随着智能汽车、智能终端、智能家居和智能制造等产业的快速发展，各应用领域出现越来越多的无线化诉求和趋势，现有的无线短距通信技术在时延、可靠性、同步精度、安全性等方面已无法满足新兴场景的演进需求。星闪联盟在此背景下成立，针对行业需求痛点提出新一代无线短距通信技术，简称为“星闪（SparkLink）”。

本白皮书分享了星闪技术的系统架构以及星闪技术在智能汽车、智能终端、智能家居和智能制造等领域的典型应用场景，并分析了星闪技术在各场景下面临的网络安全威胁和网络安全需求。为了应对这些网络安全威胁和网络安全需求，星闪技术提出了相应的网络安全机制。白皮书从网络安全架构、星闪接入层安全、星闪设备安全、星闪应用安全等方面对星闪1.0的网络安全机制进行了介绍。星闪1.0系列标准已于2021年底制定完成，其构建了基于星闪接入层、基础服务层和基础应用层在内的核心端到端架构。

针对智能汽车、智能终端、智能家居和智能制造等领域不断演进的应用需求和网络安全挑战，星闪无线短距通信技术在网络安全方面将持续演进。当前已启动星闪2.0技术的标准化工作，旨在完善网络安全技术指标，丰富网络安全技术特性，对接和适配更多行业应用和场景的网络安全需求，构建更加安全的产业生态。

目　录

缩略语

AGV	Automated Guided Vehicle	自主导航车辆
AR	Augment Reality	增强现实
ECU	Electronic Control Unit	电子控制单元
PSK	Pre-Shared Key	预共享密钥
SLB	SparkLink Basic	星闪基础接入技术
SLE	SparkLink Low Energy	星闪低功耗接入技术
VR	Virtual Reality	虚拟现实

第一章 星闪技术和应用场景介绍

1.1 星闪技术

1.1.1 概述

星闪技术是一种无线短距离通信技术，用于承载智能汽车、智能终端、智能家居、智能制造等领域应用场景的数据交互。星闪无线通信系统由星闪接入层、基础服务层以及基础应用层三部分构成，如图 1所示。其中，星闪接入层也可被称为星闪底层，基础服务层和基础应用层构成了星闪上层。

图 1 星闪无线通信系统

星闪接入层根据实现功能的不同分为管理节点（G节点）和终端节点（T节点），其中G节点为其覆盖下的T节点提供连接管理、资源分配、信息安全等接入层服务。考虑到业务场景对于无线短距离通信存在着差异化的传输需求，目前星闪接入层为星闪上层提供SLB和SLE两种通信接口。其中，SLB采用超短帧、多点同步、双向认证、快速干扰协调、双向认证加密、跨层调度优化等多项技术，用于支持具有低时延(20us)、高可靠、精同步、高并发和高安全等传输需求的业务场景。SLE采用Polar信道编码提升传输可靠性，减少重传节省功耗，同时支持最大4MHz传输带宽、最大8PSK调制，支持1对多可靠组播，支持4KHz短时延交互，安全配对，隐私保护等特性，在尽可能保证传输效率的同时，充分考虑了节能因素，用于承载具有低功耗诉求的业务场景。SLB和SLE面向不同业务诉求，提供不同的传输服务，两者相互补充并且根据业务需求进行持续平滑演进。

1.1.2 星闪技术系统架构

星闪无线通信系统的整体系统架构如图 2所示：

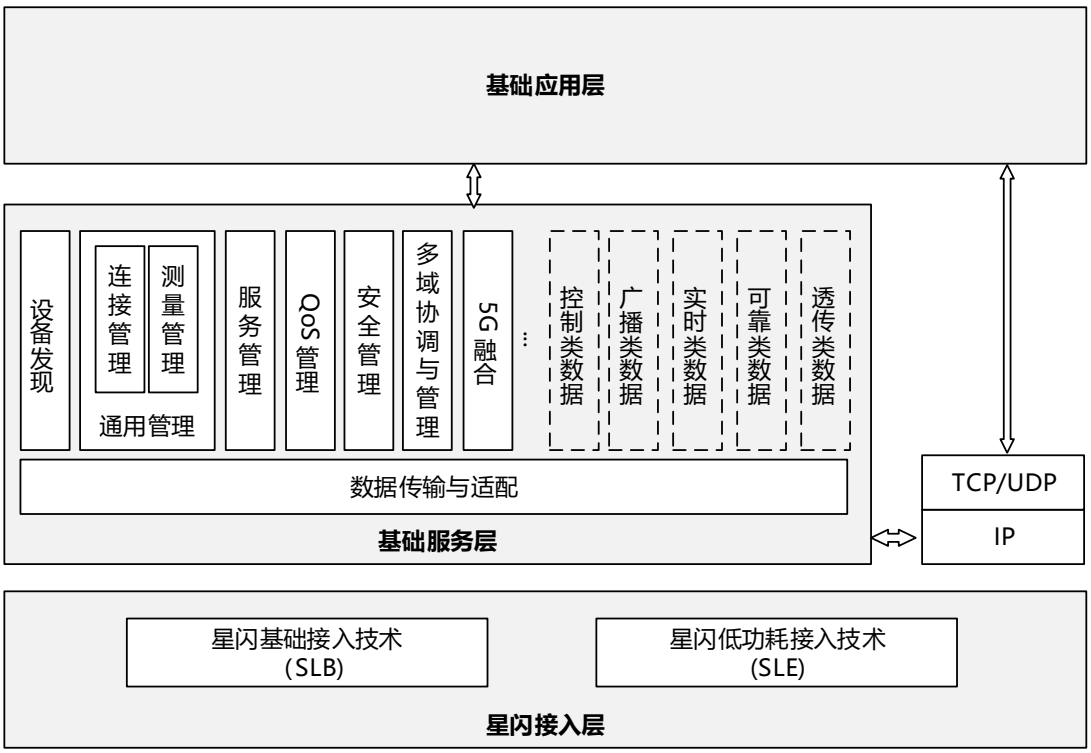

图 2 星闪无线通信系统架构

- 星闪接入层由星闪基础接入技术SLB和星闪低功耗接入技术SLE两种通信接口组成。星闪接入层为星闪上层提供的SLB和SLE两种通信接口，并为上层提供了相应的接入层安全机制。SLB信息安全定义了星闪设备间SLB安全通信所需的信息安全特征，如认证凭证配置、认证和安全参数协商、空口通信安全保护、密码算法等，提供了强认证鉴权和高信息安全的传输安全保护。SLE信息安全定义了星闪设备间SLE安全通信所需的信息安全特征，如配对和鉴权管理、安全控制、隐私管理、密码算法等，提供了数字比较、免输入、通行码输入、口令验证、带外方式和预配置密钥PSK等6种配对和鉴权方式。

- 基础服务层由一系列基础功能单元构成，星闪无线通信系统通过调用不同功能单元实现对于上层应用功能以及系统管理维护的支持。其中：设备发现功能单元、通用管理功能单元（包括连接管理、测量管理等）、服务管理功能单元、QoS管理功能单元和安全管理功能单元构成了星闪无线通信系统的无线短距通用控制面；多域协调与管理功能单元和5G融合功能单元为可选功能单元，属于星闪无线通信系统扩展控制面；数据传输与适配功能单元负责了数据封装等业务面功能，支持承载包括控制类数据、广播类数据、实时数据、可靠数据和透传数据在内的业务数据传输。安全管理功能单元提供基础服务层的信息安全服务功能，包括安全连接管理、安全状态管理、授权管理、5G融合安全管理等服务功能。安全连接管理为应用层提供建立安全连接、取消安全连接、安全连接状态查询和安全连接状态通知等服务。安全状态管理为应用层提供安全状态查询和安全状态通知等服务。授权管理提供基础服务层授权管理和基础应用层授权管理等服务。5G融合安全管理为星闪和5G蜂窝网融合场景提供安全服务。

- 为保证应用层端到端的安全，星闪定义了应用层传输安全机制和应用的安全要求，以保障端到端的应用层安全。针对基于IP的传输，星闪设备宜支持TLS/TLCP协议；针对基于Non-IP的传输，星闪设备使用的应用层传输安全机制由具体应用实现。

1.2 星闪典型应用场景

1.2.1 智能汽车典型场景

近年来，汽车的功能和使用方式正在发生深刻的变化，由单纯的交通工具转变为移动的智能空间，汽车正朝着“数据决定体验，软件定义汽车”的方向发展。当前汽车的电子电气架构不断演进，自动驾驶功能、座舱交互功能等不断丰富，高性能的控制器在增加，分布式ECU逐渐向集中式域控制器演进。传统车内有线通信技术存在成本高、部署不灵活、整备重量高等问题。当前，部分车内通信业务正呈现出从有线通信向无线通信加速演变的趋势。汽车的智能化、网联化以及无线化，给汽车网络安全也带来了巨大的风险和挑战。

典型的车内无线通信场景主要包括：

1）无钥匙进入

无钥匙进入，即一键启动系统，通过确定钥匙的位置来实现车辆的智能解、闭锁或动力系统启动。对于无钥匙进入应用，主要有如下业务需求：

– 距离测量：车辆测量钥匙或手机的距离（左前、右前、中、左后、右后距离），精度到厘米级别；

– 位置感知：有效识别车内、车外区域位置；

– 车辆钥匙功能：迎宾、自动解锁、自动闭锁（离开），车内防盗上电（自动，可根据应用需要设定功能）；

– 网络安全需求：比如防中继攻击：无线通讯信息不可截取和伪造；

– 隐私保护需求：保护用户的位置隐私。

无钥匙进入目前实现方案存在好多弊端：LF 方案无法与手机等智能终端互联，无法满足智能网联汽车的产业融合发展趋势，而蓝牙方案目前无法全面应对车载复杂工况以及定位精度需求，例如在智能设备放入口袋后常会导致功能无法正常工作。此外，这些技术也不时有“中继攻击”案例发生，安全性方面有待加强。

星闪技术具备高可靠、低时延、高速率、精同步、高安全、隐私保护、支持业务多并发以及低功耗等，可以很好的解决上述问题，提升无钥匙进入系统的业务体验。

2）车机互联

随着汽车新四化的进展以及物联网等技术的演化，车上内容、服务和体验数字化、网络化、开放

化成为趋势，车用操作系统的封闭性的现状正在逐步被打破。国内外各大厂商的车机互联产品应运而生，使得智能终端和汽车的连接越来越紧密。车机互联通过有线或无线的方式将智能终端的内容投射到车内屏幕上，主要是导航类、音频类、投屏交互类等应用场景。

为了实现无线连接以及音视频的实时传输等要求，车机互联主要存在以下业务需求：

- 音频播放类端到端时延应小于 40ms，单向时延应小于 15ms；
- 应至少支持 4 路扬声器同时工作；
- 传输音频业务速率应不小于 320kbps，宜为 1.4Mbps，可为 18Mbps；
- 投屏类业务传输的端到端时延应小于 20ms，单向时延小于 2ms；
- 应至少支持 2 路投屏，宜支持 4 路投屏；应至少支持 2 个设备分别投屏；
- 传输 1080p 视频，传输速率不小于 10Mbps；传输 720p 视频，传输速率不小于 5Mbps；
- 车载设备间单路传输可靠性（块成功率）应不低于 99.999%；
- 网络安全需求：应支持端到端的安全防护，确保车机互联业务通信的安全性；
- 隐私保护需求：应支持用户的隐私保护，包括用户车机数据、用户敏感信息等。

基于星闪技术的通信能力，车机交互在速率、连接数、可靠性、时延以及网络安全、隐私保护等方面都将获得高性能的无线短距传输通道，使能业务的极致体验。

3）营运车辆全景环视

对于大型客车或者货车等营运车辆，车身周围存在较大范围的盲区，常在车辆起步或者泊车时发生碾压盲区内的行人或非机动车辆的事故。在城区人口密集地段，这类事故风险尤为严重。当前传统的广角后视镜无法实现对车身周围盲区的全覆盖。使用全景环视系统成为解决此类安全问题的有效途径。全景环视系统可将车身周围摄像头拍摄的图像实时传递到中控平台并对多个摄像头的数据进行拼接，形成车身周围 360 度环视图像，从而实现对盲区的全覆盖。

营运车辆对于全景环视系统存在强烈的无线化诉求，具体表现在：传统客车使用空调管道部署有线进行连接，容易漏水；货车结构复杂，布线空间有限，采用有线部署的话存在着随运行时间增加可靠性降低的风险；甩挂车缺乏统一的视频接口标准用于牵引车和挂车，不同厂商之间无法适配。基于星闪技术可以很好的解决有线部署可靠性低，安装部署复杂，有线视频接口不统一的问题，并起到降低线束成本的作用，切实提升营运车辆的全景环视性功能，保障营运安全。全景环视系统的无线化给网络安全带来了挑战，需要支持摄像头身份认证、环视图像端到端安全传输等网络安全机制。

1.2.2 智能家居典型场景

随着信息化、智能化、物联化的技术发展，智能家居/智慧家庭日益普及，家庭中的智能互联设备越来越多，位置和设备种类也比较灵活多样，涉及多种信息的传递包括控制指令、音频视频、图像等内容，之前存在的痛点问题包括：

— 多音响播放不同步（同步精度要求高，us 级别）

— 多设备协同播放时音画不同步（秒级差别）

— 交互时画面、声音、操控不同步（需要控制在 ms 级别）

— 支撑未来全方位的智能家居控制、传感等，支持大量（100 个以上）设备的在线连接

基于上面面临的问题智能家居需要低时延、大带宽的可靠无线家庭内的互联技术进行互联。基于星闪技术的通信能力，智能家居在时延、速率、连接数、可靠性等方面都将获得高性能的无线短距传输通道，提升智能家居业务的消费者体验。

随着智能家居品类的增加，产品形态也呈现出多样性，设备之间通过网络交互信息的能力也越来越强。不同产品形态的设备受限于体积和成本等因素，在安全等级和支持的安全标准等方面的也存在差异，还存在支持不同接入层技术的设备混合组网的场景。在此背景下，原来作为人们最隐私的家庭环境由于智能设备的加入，智能家居设备之间交互数据，云端或设备间的数据采集和分析，整个家庭变成了网络大数据的一部分，如何保护家庭隐私值得重点关注。智能家居的数据安全采集、安全传输以及安全存储，需要一整套完整的安全隐私保护机制来实现。因此智能家居场景对无线通信技术提出了以下安全方面的技术要求：

- 完善的加密鉴权机制验证配对设备身份合法性，高效甄别非法设备，快速接入合法设备；
- 支持不同等级的接入技术安全方案，适配不同形态的智能化家居设备；
- 支持为不同接入技术提供统一的安全标准和管理机制；
- 设备之间的安全隔离机制，避免通过安全能力薄弱的设备对其他设备进行攻击。

1.2.3 智能制造典型场景

物联网、人工智能、5G 等新一代电子信息技术与制造业深度融合，正在发生着以智能制造为代表的第四次工业革命，即全面智能化的工业 4.0 时代。智能制造过程中设备、设施及系统的实时通信、以及海量传感器和人工智能平台的信息交互，和人机界面的高效交互，对通信网络有多样化的需求以及极为苛刻的性能要求，并且需要引入高可靠的无线通信技术。高可靠无线通信技术在工厂的应用来看，一方面，生产制造设备无线化使得工厂模块化生产和柔性制造成为可能。另一方面，因为无线网络可以使工厂和生产线的建设、改造施工更加便捷，并且通过无线化可减少大量的维护工作降低成本。智能制造的无线化对网络安全和数据安全也提出了较高要求，包括设备的数据安全采集、数据安全传输以及安全存储等。

第二章 星闪技术面临的网络安全威胁和网络安全需求

2.1 网络安全威胁

2.1.1 传输安全威胁

星闪技术属于无线通信技术领域，在传输过程中会遭受安全威胁，主要的传输安全威胁包括：身份仿冒、伪造信息、重放或篡改信息、拒绝服务攻击、窃听数据等。同时，也面临中继攻击等更为隐蔽的攻击方式，在中继攻击中双方的通信是由攻击者发起的，攻击者只是在双方之间中继消息，而不操纵消息，甚至不一定读取消息。如针对汽车无钥匙进入场景，攻击者将通信信号从数字钥匙中继到汽车上，让汽车误以为车主在旁边从而打开车门。潜在的传输安全威胁如表 1 所示。

表 1 潜在传输安全威胁

攻击目标	攻击方法	描述
星闪通信系统	身份仿冒	仿冒身份与对端设备进行通信。
	伪造信息	向设备发送伪造的传输信息，欺骗对端设备。
	重放、篡改信息	造成对端设备无法识别正常信息。
	拒绝服务攻击	注入干扰信息，以耗尽通信信道容量，使其无法工作。
	窃听数据	通过监听等方式，窃取正常通信数据。
	中继攻击	双方的通信由攻击者发起，攻击者在双方之间中继消息，而不操纵消息。

2.1.2 设备安全威胁

星闪技术以芯片或嵌入式方式部署在车端、移动端、物联网等设备中，将面临设备安全威胁，主要包括：1. 将设备拆解下来对其进行固件提取，然后逆向分析；2. 对固件没有进行安全校验或者校验方法被绕过，可刷入被篡改过的固件，造成严重后果；3. 控制设备发送非法数据，发起拒绝服务攻击，造成设备通信拥塞无法正常工作；4. 对设备进行侧信道攻击来获取设备中的信息，如密钥等。潜在的设备安全威胁如表 2 所示。

表 2 潜在设备安全威胁

攻击目标	攻击方法	描述
星闪设备系统	固件提取、逆向分析	将设备拆解下来对其进行固件提取，并进行逆向分析。
	刷写固件	通过工具本地或远程升级刷写篡改固件，使其操作异常或无法正常工作。

	拒绝服务攻击	控制设备发送非法数据，造成通信拥塞，无法正常工作。
	侧信道攻击	基于从密码系统的物理实现中获取的信息。

2.1.3 应用安全威胁

星闪技术做为下一代无线短距通信技术，基于此通信技术可支撑上层应用完成很多功能，如车载主动降噪、无钥匙进入、车机互联等。这些应用在使用星闪技术过程当中也面临应用安全威胁，比如攻击者通过应用重打包，可向应用插入恶意代码，实现劫持等功能；攻击者可以绕过鉴权机制，越权访问应用；攻击者能够通过调试或者反编译方式来获取通信密钥、分析通信协议，并结合应用相关功能来伪造指令，干扰用户使用。潜在的应用安全威胁如表 3 所示。

表 3 潜在应用安全威胁

攻击目标	攻击方法	描述
星闪应用	应用重打包	通过应用重打包，可向应用插入恶意代码，实现劫持等功能。
	攻击鉴权机制	越权访问应用。
	反编译攻击	获取代码进行逆向分析。

2.2 网络安全需求

星闪技术安全需求主要包括传输安全需求、设备安全需求和应用安全需求。

传输安全需求

针对传输方面的安全需求，主要方面有：要对通信双方信息进行加密传输，保障通信数据的机密性；通过数据校验机制，保证重要信息的真实性；能够有对信息的过滤机制或黑白名单机制，保证信息的有效性。

设备安全需求

针对设备方面的安全需求，主要方面有：能够采取安全启动技术，在设备启动各个阶段对启动过程进行安全校验；能够有物理隔离的安全域来放置密钥；能够通过加壳混淆等多元化技术组合对代码进行加固，防止逆向破解。

应用安全需求

针对应用方面的安全需求，主要方面有：通过代码加固、调试注入防护等方式提升应用安全水平；应用访问权限控制，防止应用被越权访问；对应用进行统一安全策略管理和配置。

第三章 星闪网络安全机制介绍

3.1 星闪网络安全概述

星闪无线短距通信系统是一个全周期防护的高安全无线短距通信系统。星闪网络安全机制为星闪系统提供了高安全规格、强认证机制和全面安全防护，如表 4 所示。

1）高安全规格：星闪使用了业界主流的安全算法，包括 ZUC、SM4 和 AES 等；星闪的会话密钥采用动态协商协商的机制，同时支持前向安全；星闪网络安全机制可灵活的协商安全配置，以满足不同场景的业务需求。

2）强认证机制：星闪 SLB 使用强制双向认证，只有双向认证成功后才能建立连接，防止非法设备接入；星闪 SLE 支持静态口令和 PSK 认证，认证强度得到提高。

3）全面安全防护：星闪定义了系统实现所需的安全需求，全面保护星闪系统安全；星闪提供了全栈的安全设计，包括传输安全、设备安全和应用安全。

表 4 星闪网络安全概述

星闪网络安全概述	安全要求举例
高安全规格	• 业界主流安全算法：ZUC、SM4、AES • 动态会话密钥协商，支持前向安全 • 安全机制可协商灵活安全配置，满足业务需求
强认证机制	• SLB强制双向认证：双向认证后才能建立连接，防止非法设备接入 • SLE支持静态口令、动态口令和PSK认证，提高认证强度
全面安全防护	• 定义系统实现安全需求，全面保护星闪系统安全 • 全栈安全设计：设备安全、传输安全、应用安全

3.2 星闪网络安全架构

星闪接入层为星闪上层提供 SLB 和 SLE 两种通信接口以及相应的接入层安全机制。SLB 接入层提供认证和安全上下文协商、隐私管理和加解密等接入层安全机制。SLE 接入层提供配对和鉴权管理、隐私管理和加解密等接入层安全机制。

基础服务层针对上层业务数据提供服务功能，其中基础服务层的安全管理功能单元提供基础服务层的网络安全服务功能，包括安全连接管理、安全状态管理、权限管理、5G融合安全管理等服务功能。

基础应用层用于实现各类应用功能，基础应用层针对共性的业务诉求，可以定义通用应用服务框架。基础应用层可以提供应用层传输安全机制以实现端到端的应用层传输安全。

为了提高星闪无线通信系统抵抗攻击的能力，星闪无线通信终端设备应满足设备安全要求，包括安全存储、安全执行、安全防护和安全管理等方面。

星闪安全架构包含以下安全域，如图 3 所示：

- 传输安全：设备间安全通信所需的安全特征，如认证凭证配置、双向认证、安全上下文协商和更新、传输数据安全保护、隐私保护等。提供强认证鉴权和高安全的传输安全保护。
- 设备域安全：设备需要支持的安全特性，如安全存储、安全执行、安全防护、安全管理等。支持安全存储和分域安全隔离等机制。
- 应用域安全：应用层的安全特性，包括应用层传输安全机制、使用星闪的应用需要满足的安全需求等。可根据业务特征，配置应用、传输、设备安全机制规格。

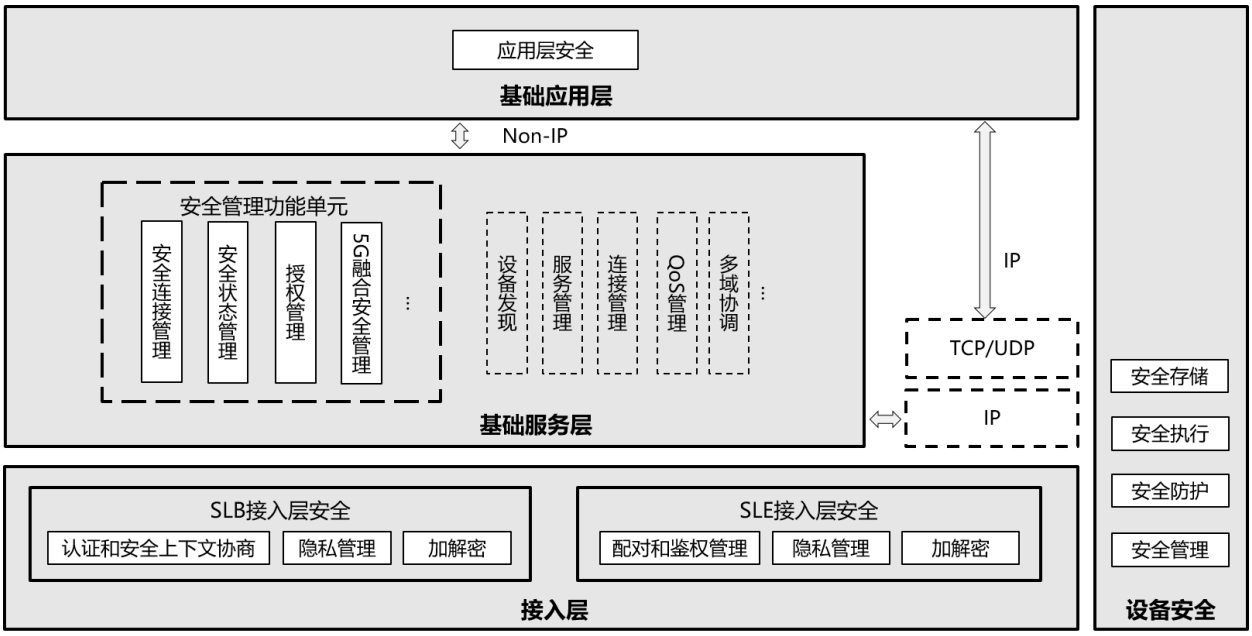

图 3 星闪无线通信系统安全架构

3.3 星闪接入层安全

3.3.1 星闪基础接入技术（SLB）安全

1） 认证凭证配置

认证凭证配置用于在 G 节点和 T 节点之间配置相同的 256 比特共享密钥 PSK。星闪支持三种配置方案：

- 配置密钥方法：通过预配置的方法，将256比特共享密钥PSK预配置在T节点和G节点上。
- 配置口令方法：用户在G节点和T节点上输入相同的口令。口令通过密码算法转换为256比特共

享密钥PSK。

- 第三方服务器认证凭证配置方法：G节点和T节点获取到应用服务器发送的认证口令，基于认证口令获得256比特PSK。

通过以上三种配置方法，T节点和G节点之间可以配置相同的256比特密钥PSK。

2） 认证和安全参数协商

认证凭证配置完成之后，G 节点和 T 节点应基于配置的认证凭证（256 比特密钥 PSK）执行双向身份认证，双向身份认证机制基于挑战/应答的方法。

G 节点和 T 节点在双向身份认证的同时协商安全参数，如协商加密算法、完整性保护算法、加密密钥和完整性保护密钥。加密算法和完整性保护算法的协商基于双方的安全能力协商出优先级最高的算法。加密密钥和完整性保护密钥从密钥协商算法（SM2、ECDH）得到的主密钥推演而来。

G 节点和 T 节点可配置白名单，只有白名单中的设备才能建立关联。G 节点和 T 节点也可配置黑名单，当认证失败次数超过阈值时锁定用户。

星闪支持隐私保护机制，G 节点和 T 节点建立关联之后，G 节点给 T 节点分配临时 ID。T 节点在下次关联时使用该临时 ID 作为 T 节点身份。

3） 空口通信安全保护

认证和安全参数协商完成之后，G 节点和 T 节点基于协商的安全参数（密码算法、密钥等）对空口通信进行安全保护。星闪支持密钥更新机制，密钥有效期到期或新鲜性参数重复之前，G 节点触发密钥更新流程更新 G 节点和 T 节点之间密钥。

4） 密码算法

星闪 SLB 支持加密算法、完整性保护算法、密钥协商算法和密钥派生函数。每一类算法都支持国密算法和国际算法。

3.3.2 星闪低功耗接入技术（SLE）安全

1） 配对和鉴权管理

星闪SLE支持六种配对和鉴权方式：

- 数字比较

比较G节点和T节点上显示的数字是否一致。

- 通行码输入

一个设备显示一组数字，另外一个设备通过键盘输入该数字。

- 口令验证

用户在G节点和T节点的用户界面上输入相同的满足复杂度要求的数字或字符的组合（口令）。

- **带外方式**

通过额外技术进行身份鉴权，如NFC。

- **PSK方式**

将256比特共享密钥PSK预配置在G节点和T节点上，G节点和T节点基于该PSK进行身份鉴权。

- **免输入**

G节点和T节点直接配对，不能支持抗中间人攻击。建议使用该方式时做些限制，比如需要用户按特定按键。

需要说明的是，免输入不能支持抗中间人攻击，需谨慎使用。如果使用免输入配对，建议在应用层做些限制，比如：只有在用户按特定按键的时候，或者只有确认对端设备在近距离的时候，才进入这种配对状态。

2） 安全控制

配对和鉴权管理完成之后，G 节点和 T 节点开始启动安全控制流程对空口通信进行安全保护。安全控制流程包括启动安全流程和暂停安全流程。

启动安全流程开始后，G 节点和 T 节点都需要将本地的用户数据和其他控制消息的收发暂停发送。G 节点和 T 节点协商会话密钥，后续将在安全状态下继续用户和其他控制消息的收发。

暂停安全流程的目的是重新生成连接的会话密钥，以支持在不断开连接的情况下对通信双方的密钥进行动态刷新，从而实现更好的安全性。

3） 隐私管理

星闪SLE提供对系统真实身份的隐藏，避免恶意的服务器或监听者能收集星闪无线低功耗系统的私有数据，并防止被跟踪。

G节点和T节点身份认证成功之后，G节点分发可解析地址密钥给T节点。G节点和T节点基于可解析地址密钥生成以及解析可解析随机标识，从而保护G节点和T节点的隐私。

4） 密码算法

星闪SLE支持加密算法、完整性保护算法、密钥协商算法和密钥派生函数。每一类算法都支持国密算法和国际算法。

3.4 星闪设备安全

为了提高星闪无线通信系统抵抗攻击的能力，星闪定义了星闪无线通信终端设备应满足的设备安全要求，包括安全存储、安全执行、安全防护和安全管理理等方面，如表 5所示。

星闪设备应支持敏感信息的安全存储，防止敏感信息泄露或篡改。敏感信息包括密钥、口令、用户身份、安全上下文、白名单、黑名单等。星闪设备存储不同用户的数据时，应支持不同用户数据的安全访问控制机制。星闪设备的安全敏感操作（如加密、解密、完整性验证等）应在安全环境中执行。同时建议支持安全启动。星闪设备的调试接口应在上市产品中禁用或进行安全访问控制。同时应该禁用闲置的物理端口。星闪设备应支持安全事件的安全日志记录功能和安全日志的安全存储。同时不应存在CNVD和CNNVD等漏洞平台已公开发布的6个月以上的高危及以上等级漏洞。

表 5 设备安全要求

设备安全	安全要求举例
安全存储	• 敏感信息安全存储 • 用户数据的访问控制，防止未授权访问
安全执行	• 安全敏感操作应在安全环境中执行 • 宜支持安全启动
安全防护	• 调试接口禁用或进行安全访问控制 • 禁用闲置的物理端口
安全管理	• 安全日志记录 • 安全日志的安全存储 • 不应存在已公开发布6个月以上的高危及以上等级漏洞

3.5 星闪应用安全

针对星闪应用安全，星闪定义了应用层传输安全机制和应用的安全要求，同时星闪可进行应用专属的安全设置，可根据业务特征配置安全机制。典型应用场景下的安全配置示例如表 6所示。

表 6 应用安全要求

典型应用场景	安全配置建议
降噪	• 认证凭证配置：配置密钥方法； • 传输安全保护：关闭用户面完整性保护；可开启用户面加密保护； • 安全隔离：禁止车载无线短距通信系统的流量进入车内网。
语音	• 认证凭证配置：配置口令方法； • 传输安全保护：可开启用户面完整性保护和加密保护； • 安全隔离：禁止车载无线短距通信系统的流量进入车内网。
投屏	• 认证凭证配置：配置口令方法； • 传输安全保护：可开启用户面完整性保护和加密保护； • 安全隔离：禁止车载无线短距通信系统的流量进入车内网。
电子钥匙	• 认证凭证配置：配置密钥方法；

	• 传输安全保护：必须开启用户面机密性和完整性保护； • 安全隔离：允许车载无线短距通信系统的流量进入车内网。

第四章 星闪网络安全特性总结和未来规划

4.1 星闪网络安全特性总结

星闪SLB网络安全在极简和高安全方向做了增强设计，具有网络安全特性如表 7所示。

表 7 星闪 SLB 网络安全特性

SLB网络安全特性	说明
信令数量极简	网络安全机制融入到关联流程中，信令数量极简： • 无网络安全上下文场景5条信令； • 有网络安全上下文场景3条信令。
高强度凭证	认证凭证配置机制提供了高强度的认证凭证，口令复杂度要求标准化。
强认证鉴权	强制的双向身份认证机制提供了强认证鉴权的网络安全能力，未认证的设备被禁止接入。
双密码算法	• 密码算法支持128bit密码算法ZUC和AES； • 密钥架构中所有对称密钥长度为256比特； • 双密码算法在汽车长生命周期内提供双保险，避免一破通破。
加密、完保独立on/off	• 算法协商机制支持加密和完整性保护算法的协商，方便后续引入新的算法； • 根据业务场景需求，加密和完整性保护可独立开启或关闭。
黑白名单防护	• 白名单防护机制根据前装设备确定关联集合，禁止集合外设备接入； • 黑名单机制提供认证失败次数超过阈值时锁定用户的能力； • 黑白名单机制减少了DoS攻击风险。

星闪SLE网络安全在强口令认证和高安全方向做了增强设计，具有网络安全特性如表 8所示：

表 8 星闪 SLE 网络安全特性

SLE网络安全特性	说明
强口令认证	• 同时支持静态口令和动态口令，提高安全性，简化信令流程。
免输入安全增强	• 实现免输入配对时必须增加安全加固措施（如用户手工操作设备进入配对模式、配对距离限制等）； • PSK配对部分替代免输入配对，支持无输入无输出能力设备连接场景：双方支持配置PSK时，预配置PSK，基于PSK进行配对和鉴权。
双密码算法	• 密码算法支持128bit密码算法SM4和AES； • 双密码算法在汽车长生命周期内提供双保险，避免一破通破。
加密、完保独立开关	• 算法协商机制支持加密和完整性保护算法的协商，方便后续引入新的算法；

	• 根据业务场景需求，加密和完整性保护可独立开启或关闭。

4.2 星闪网络安全未来规划

随着数字世界的不断发展，信息在人、物、环境之间的循环流转让连接变得无可或缺，智能汽车、智能终端、智能家居和智能制造等领域的新兴应用场景不断涌现，相应的业务需求对传统无线短距通信技术在网络安全方面提出了严峻的挑战，产业亟需能够满足新业务需求和发展趋势的安全技术。

着眼于星闪无线短距通信技术未来发展和安全需求，针对星闪未来发展可能面临的网络安全新形势和新需求，建议从完善安全技术标准、构建有效的安全防护体系、探索和研究安全新技术新应用、建立并完善漏洞分享机制等多个维度着手，联合行业伙伴力量，共同打造星闪安全生态。

以此为目标，星闪联盟将：

1、结合网络安全应用场景的需求演进，持续推动星闪网络安全创新研究，针对重点网络安全问题开展技术攻关，要进一步理清不同应用场景的网络安全风险，设立专题攻关任务，联合行业共同突破，要建立发现问题和解决问题的能力体系。

2、构建星闪安全技术标准体系，形成星闪安全系列标准，重点开展安全通用要求、评价方法、测试方法、事件处置等核心标准研制工作。联盟现已启动星闪 Release 2.0 的标准化工作，在星闪网络安全领域，将在高精定位安全、合作设备集合管理安全、SLE 设备安全要求与测试方法等安全方向进行重点增强。

3、加速推动星闪 Release 1.0 安全技术的产品落地和实际商用。推动解决方案、测试认证等环节，推动星闪安全技术在四大领域的高价值场景中率先实现规模商用。

4、建立并完善漏洞分享机制，及时处理星闪遇到的网络安全问题，不断提高星闪产品的安全性。