SparkLink

# 星闪无线短距通信技术
# 应用场景网络安全解决方案

2023 年 12 月

# 版权声明

# 目　录

# 第一章 无线短距通信技术痛点场景和星闪短距技术介绍

## 1.1 无线短距通信技术痛点场景

高质量的网络连接将驱动智能汽车、物联网和工业互联网发展，结合云计算和人工智能，创造全新的经济生态、关键基础设施、生产制造和服务体系、新型应用和消费模式，在此过程中，会产生新的应用场景和需求，由此对无线短距通信技术提出了新的要求和挑战。随着智能汽车、智能家居、智能终端和智能制造等产业的发展，创新需求和应用不断涌现，星闪无线短距通信技术（以下简称星闪短距技术）的部分新应用和业务如图 1所示。

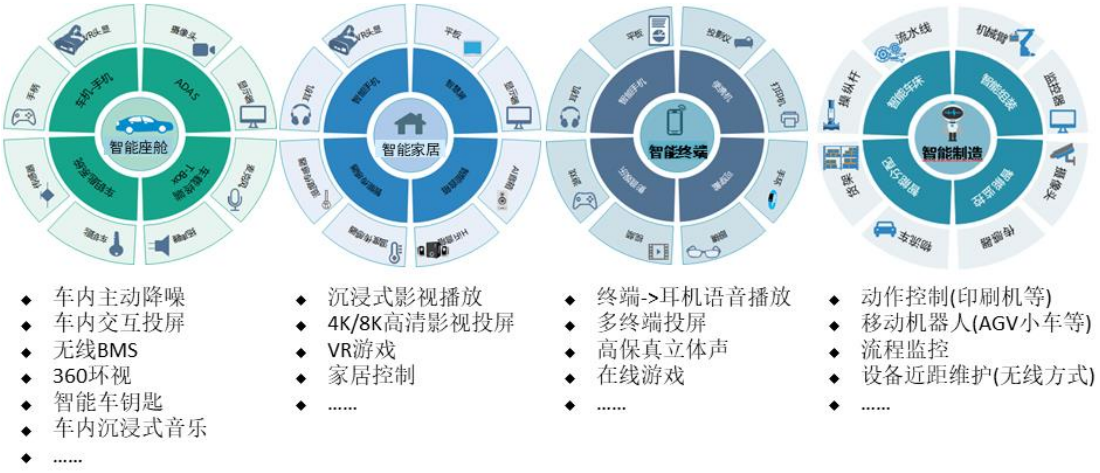


图 1 星闪技术应用场景示例

随着新场景的不断涌现，包括智能汽车、智能家居、智能终端和智能制造在内的多应用领域在低时延、高可靠、精同步、高速率、多并发、高信息安全和低功耗等方面都对无线短距通信技术提出了更高的通信要求。现有主流无线短距通信技术存在某些技术性能的先天局限，如抗干扰性、QoS和通信时延，或者在某些方面的技术潜力已靠近天花板，如可靠性和高密度部署，导致其无法满足新应用的技术要求：

1. 智能汽车对无线短距有低时延、高安全、高可靠抗干扰等要求：以新能源汽车的电池管理系统为例，电池管理系统对全车电池组进行安全监控和充放电过程控制，由于现有无线短距通信技术在管理终端数量、时延和可靠性等方面都不满足要求，只能求助于有线方案，但又面临着增加电池重量、降低电池包密度、影响测量精度和维护成本上升等困难。同时，车载应用要求高可靠性和高安全性，以应对车内外复杂的电磁干扰环境以及潜在的网络安全攻击，而现有无线短距通信技术基于竞争性的无线资源使用、消费类安全保障机制和大量设备连接，存在明显的能力短板。

2. 智能家居对无线短距有中高业务速率、高质量抗干扰、低时延精同步、高安全保障等要求：以客厅为入口的智能家居逐渐成为家庭网络中心，智能音箱、智能电视以及其它智能家电之间的互动连

接应用逐渐普及。家居场景通信对于数据传输的安全可靠以及隐私保护也有高要求，随着家庭WiFi和蓝牙设备的增加，室内干扰增加，对传输可靠性也提出挑战。

3. 智能终端对无线短距有可穿戴终端的高密度接入的抗干扰、低时延业务、高安全保障等要求：以智能手机、手表手环、耳机、笔记本和平板电脑为代表的智能终端已逐渐成为人们办公、娱乐和学习的常见设备。其中，多屏协同实现手机和笔记本/平板电脑之间的同步操作，以及手机、电视和手柄等智能设备之间联合操控进而带来沉浸式娱乐体验，已经成为智能终端黏着用户的主要卖点特性。在这类场景下，保证多设备的高精度同步和毫秒级低时延需要，同时兼顾高速率大数据量的音视频传输和小数据低速率的业务控制，以及多设备之间干扰规避，已经成为痛点问题。可穿戴设备，尤其是耳机和手环等日益成为消费热点，受设备体积限制，需要同时满足高质量音频传输（中等速率）、组播、低时延操作类业务交互、抗干扰和苛刻的功耗需求，传统短距技术多考虑单一或少数性能的极限优化，很难兼顾。同时，智能终端之间的网络安全也有较高要求，包括设备认证、数据安全传输和隐私保护等。

4. 智能制造对无线短距有超低时延、精准同步、高可靠性、高安全等要求：工业互联网需要结合低时延、高可靠、大带宽、广覆盖、可定制的工业企业外网和确定时延、精细调度、智慧运维的工业企业内网，融合IT技术与OT技术，使能柔性制造，满足消费者大量的分散的个性化需求，最终打破产业链数据孤岛，形成数据驱动的企业运营和业务模式创新。对于工业企业内网，当前大部分工厂普遍采用有线网络连接方案以保证低时延、高可靠、高安全的需求，有线连接存在初装成本高、可扩展性差和移动性不足等问题。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。

基于上述分析，智能汽车、智能家居、智能终端和智能制造等领域对于无线短距通信提出了超低时延、高可靠、抗干扰、高安全、精准同步等共性要求，而现有短距无线技术在这些维度存在显著的性能差距。

## 1.2 星闪短距技术介绍

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 2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 2 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、加密保护、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。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。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。

# 第二章 星闪关键场景网络安全分析

## 2.1 智能汽车场景

根据 YD/T 4007-2022《无线短距通信 车载空口技术要求和测试方法》，星闪基础接入技术 SLB 的关联流程中认证凭证配置方法包括配置密钥方法：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。根据 T/XS 10002-2022《星闪无线通信系统 接入层 低功耗技术要求和测试方法》，星闪低功耗接入技术 SLE 支持预共享密钥 PSK 鉴权。

因此星闪基础接入技术 SLB 和星闪低功耗接入技术 SLE 均可以基于预共享密钥 PSK 建立星闪连接。此时，设备中需要预配置共享密钥 PSK，例如针对智能汽车的前装设备，厂商可以在前装设备中预配置共享密钥 PSK。但如何配置预共享密钥 PSK 在标准 YD/T 4007-2022《无线短距通信 车载空口技术要求和测试方法》和 T/XS 10002-2022《星闪无线通信系统 接入层 低功耗技术要求和测试方法》中没有定义。本文件将给出几种预配置共享密钥 PSK 的方案。

完成共享密钥 PSK 预配置之后，不同的智能汽车场景基于 PSK 可能使用不同的网络安全机制，如无线电池管理系统（wBMS）适合使用基于 SLE 的网络安全机制。本文件还将针对智能汽车的典型场景，即无线电池管理系统（wBMS），给出网络安全解决方案。

## 2.2 智能终端场景

根据 YD/T 4007-2022《无线短距通信 车载空口技术要求和测试方法》，星闪基础接入技术 SLB 的关联流程中认证凭证配置方法包括：

- 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。

针对智能终端场景，由于智能终端可能会和其他任意的终端建立星闪连接，因此在两个建立星闪连接的任意智能终端上预配置密钥较难实现。同时针对无输入无输出的设备（即弱能力设备），用户无法在设备上直接输入口令。因此针对弱能力设备，如何配置认证凭证是一个难点，标准中也没有定义。本文件将给出几种智能终端场景弱能力设备口令配置的方案。

# 第三章 智能汽车场景密钥管理解决方案

## 3.1 概述

本章节将给出几种智能汽车场景密钥管理解决方案，包括配置共享密钥 PSK 方案和更换部件时的配置共享密钥 PSK 方案。

## 3.2 配置共享密钥 PSK 方案

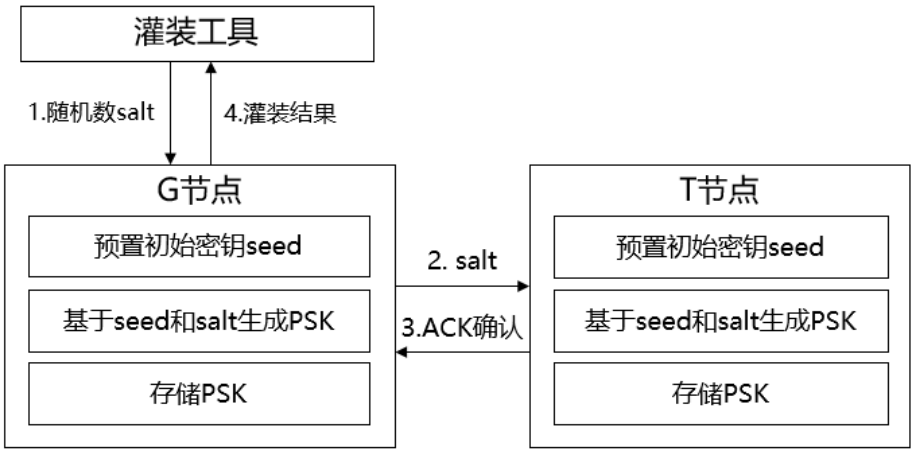


图 3 配置共享密钥 PSK 方案

配置共享密钥 PSK 方案如图 3 所示。在 G 节点和 T 节点中都预置初始密钥 seed，例如厂商可以在星闪芯片中预置初始密钥 seed。G 节点和 T 节点基于预置的 seed 和获得的随机数 salt 生成共享密钥 PSK，流程描述如下：

1、灌装工具生成一个随机数 salt。灌装工具把该随机数 salt 发送给 G 节点。随机数 salt 可通过有线或者无线（例如，星闪）的方式发送给 G 节点。

2、G 节点把随机数 salt 发送给 T 节点，可通过有线或者无线（例如，星闪）的方式发送。

3、T 节点收到随机数 salt 之后，T 节点基于预置的初始密钥 seed 和随机数 salt 推演 PSK，PSK=KDF (seed, salt)。KDF 表示密钥派生函数，如 HMAC-SM3、HMAC-SHA256。T 节点发送确认消息给 G 节点。

4、G 节点基于预置的初始密钥 seed 和随机数 salt 推演 PSK，PSK=KDF (seed, salt)。

G 节点和 T 节点保存 PSK，用于后续建立星闪连接。

seed 的长度建议为 256 比特，salt 的长度建议为 256 比特。PSK 的长度建议为 256 比特。

针对不同的场景，seed 的粒度可以不同。比如汽车场景，seed 的粒度可以是一个车型一个 seed。终端

场景，seed 的粒度可以是一个型号一个 seed。

### 3.3 更换部件时的配置共享密钥 PSK 方案

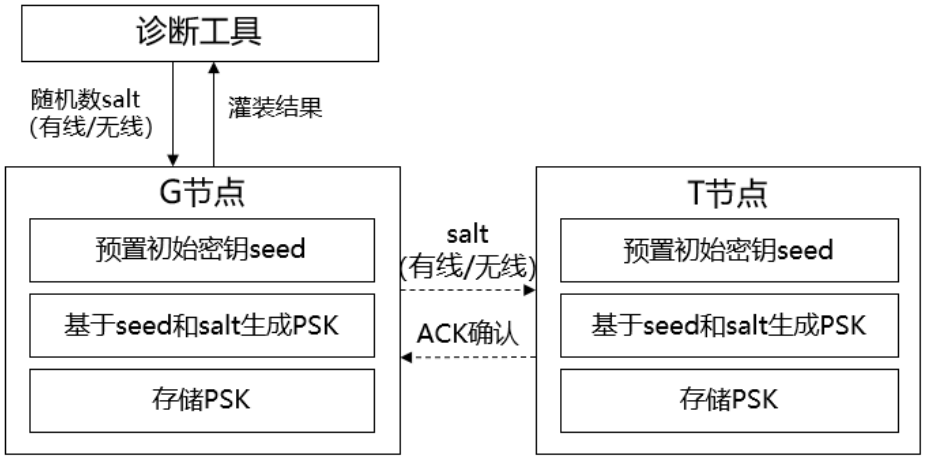


图 4 更换部件时的配置共享密钥 PSK 方案

当部件需要更换时，需要在新部件中重新配置共享密钥 PSK，方案如图 4 所示。诊断工具可以从厂商处获取随机数 salt，如可以通过远程方式获取。更换的 G 节点或 T 节点中都预置初始密钥 seed，配置共享密钥 PSK 流程描述如下：

更换 G 节点：

1、诊断工具给 G 节点发送随机数 salt。随机数 salt 可通过有线或者无线（例如，星闪）的方式发送给 G 节点。

2、G 节点基于预置的初始密钥 seed 和随机数 salt 推演 PSK，PSK=KDF (seed, salt)。G 节点保存 PSK。

更换 T 节点：

1、诊断工具给 G 节点发送随机数 salt。随机数 salt 可通过有线或者无线（例如，星闪）的方式发送给 G 节点。

2、G 节点把 salt 发送给 T 节点，可通过有线或者无线（例如，星闪）的方式发送。

3、T 节点收到随机数 salt 之后，T 节点基于预置的初始密钥 seed 和随机数 salt 推演 PSK，PSK=KDF (seed, salt)。T 节点发送确认消息给 G 节点。T 节点保存 PSK。

# 第四章 无线电池管理系统（wBMS）网络安全解决方案

## 4.1 wBMS 网络安全需求和解决方案

wBMS 面临节点数量众多、关联关系复杂、场景众多等复杂问题，需要从 wBMS 全生命周期考虑网络安全，具体 wBMS 全生命周期网络安全需求如下：（1）电池包生产过程中，需建立电池包与电池模组的安全配对关系，确保密钥灌装过程安全。（2）电池包工作过程中，需满足双向身份认证、机密性保护、完整性保护、抗重放攻击等安全通信需求。（3）电池包换电、仓储阶段，更换管理节点时，保证管理节点和电池模组之间的双向身份认证和安全通信。（4）电池包维修场景下，新电池模组与电池包建立关联关系的过程需保障网络安全。

针对以上 wBMS 全生命周期各个场景的网络安全需求，提出的网络安全解决方案如下表所示：

| 场景 | 方案 |
| --- | --- |
| **电池包生产过程** | **灌装内容**<br>• 灌装初始密钥 seed 和随机数 salt，基于章节 3.1 使用 seed 和 salt 生成 PSK）<br>**Seed 和 PSK 粒度**<br>• 一车型一个 seed<br>• 一车一个 PSK 或一车型一个 PSK<br>**灌装方式**<br>• 电池产线灌装 seed，电池产线/整车产线触发生成 PSK<br>**PSK 的存储**<br>• 建议使用 HSM 存储 PSK；<br>• 若没有 HSM，可将 PSK 存储在存储区，通过口令等方式限制读写 |
| **电池包工作过程** | 电池包工作时基于星闪接入层网络安全机制建立安全通信连接（见章节 4.2），可满足双向身份认证、机密性保护、完整性保护、抗重放攻击等安全通信需求。 |
| **电池包换电、仓储阶段** | **换电站 G 节点和电池包建立连接**<br>• 换电站配置每个车型的 seed，seed 应安全存储<br>• 当换电站需要和某电池包连接时，换电站向车企获取该电池包的 salt，换电站基于 seed 和 salt 生成 PSK |
| **电池包维修阶段** | **场景 1：G 节点损坏，更新 G 节点**<br>维修方法 1：车厂灌装密钥。<br>• 方式 1：车厂将该车的 salt 灌装到新的 BCU，车厂更换新的 BCU；<br>• 方式 2：车厂把新的电池寄给维修店，维修店进行更换。<br>维修方法 2：维修店灌装密钥。<br>• 维修店工具从车云获取该车的 salt，维修店工具把 salt 发送给 |

| | |
|---|---|
| | BCU（有线），BCU 生成 PSK。<br><br>**场景 2：T 节点损坏，更新 T 节点**<br>维修方法 1：车厂灌装密钥。<br>• 方式 1：车厂将该车的 salt 灌装到新的电芯，车厂更换新的电芯；<br>• 方式 2：车厂把新的电芯寄给维修店，维修店进行更换。<br>维修方法 2：维修店灌装密钥。<br>• 维修店工具从车云获取该车的 salt，维修店工具把 salt 发送给 BCU（有线），BCU 把 salt 发送给电芯（无线），BCU 生成 PSK。 |

4.2 wBMS 安全通信解决方案

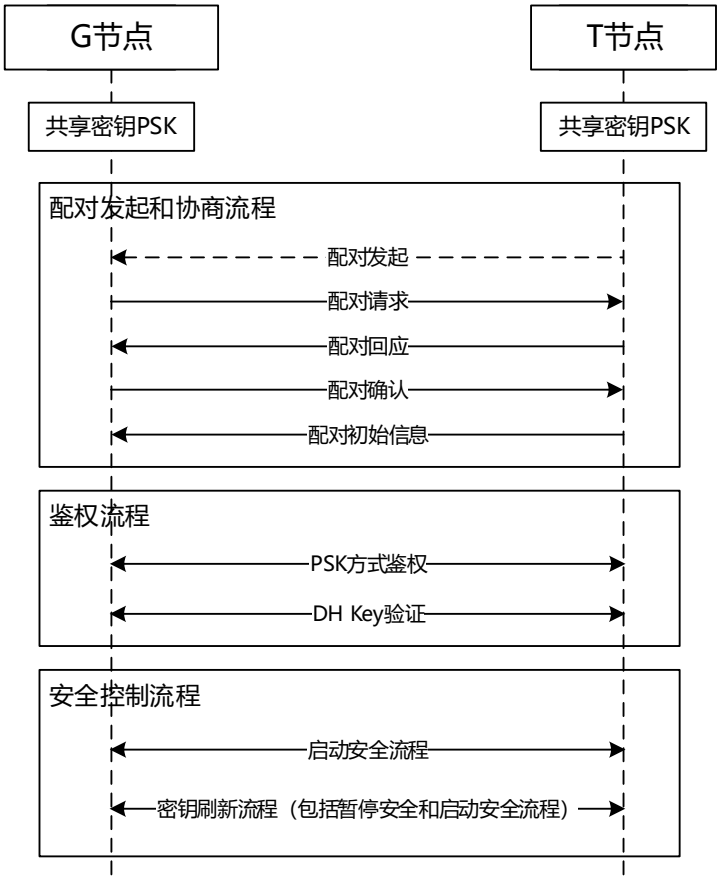


图 5 wBMS 场景的星闪 SLE 技术配对鉴权流程

wBMS 适合采用星闪 SLE 技术。星闪 SLE 技术支持 6 种配对流程，包括：数字比较、通行码输入、口令验证、带外方式、PSK 方式、免输入方式。根据 wBMS 部件的无输入无输出特性以及高安全需求，推荐使用 PSK 方式进行配对和鉴权，如图 5 所示，其中消息格式参考 T/XS 10002-2022《星闪无线通信系统 接入层 低功耗技术要求和测试方法》

# 第五章 智能终端场景弱能力设备口令配置解决方案

## 5.1 概述

本章节将给出弱能力设备的几种口令配置的方案，包括基于中心设备的弱能力设备口令配置方案和弱能力设备口令直接配置方案。

## 5.2 基于中心设备的弱能力设备口令配置方案


图 6 基于中心设备的弱能力设备口令配置方案

基于中心设备的弱能力设备口令配置方案如图 6 所示。中心设备为可以辅助弱能力设备之间建立星闪 SLB 关联的的设备，如手机、电视等。图 3 中弱能力设备以音响为例，中心设备以手机为例进行说明，流程描述如下：

1. 厂商在弱能力设备上标记二维码或口令，中心设备通过扫描二维码或者输入口令的方式获取弱能力设备的口令，手机和弱能力设备 1 以及弱能力设备 2 分别建立 SLB 关联。
2. 用户在中心设备上输入将两个弱能力设备进行关联的指令，如将中心设备界面上显示的两个弱能力设备碰到一起。
3. 中心设备从弱能力设备 1 处获取弱能力设备 1 的 SLB 口令（该 SLB 口令可以和步骤 1 中的弱能力设备 1 的口令相同，也可以不同），并把弱能力设备 1 的 ID 和 SLB 口令发送给弱能力设备 2。或者中心设备生成一个 SLB 口令，并把该 SLB 口令发送给弱能力设备 1 和弱能力设备 2。

4. 弱能力设备 2 保存弱能力设备 1 的 ID 和 SLB 口令，弱能力设备 1 和弱能力设备 2 基于 SLB 口令进行 SLB 关联。

### 5.3 弱能力设备口令直接配置方案

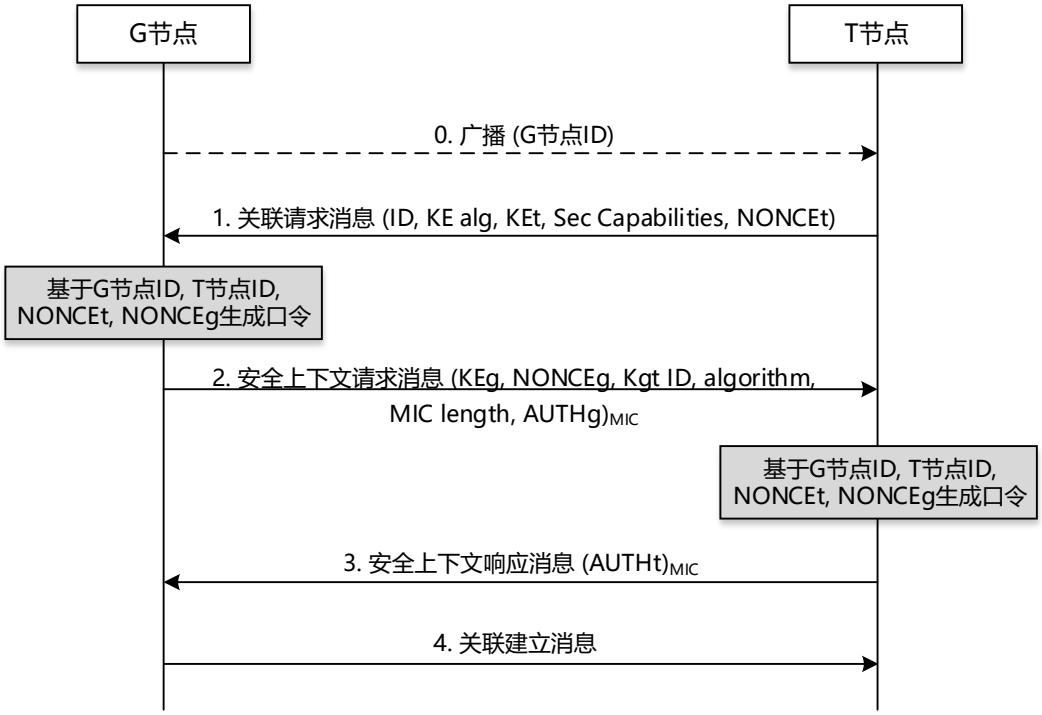


图 7 弱能力设备口令直接配置方案

基于弱能力设备口令直接配置方案如图 7 所示。基于 YD/T 4007-2022《无线短距通信 车载空口技术要求和测试方法》章节 9.3.2，在认证和安全上下文协商过程中，使用 G 节点和 T 节点的 ID 以及随机数 NONCEt 和 NONCEg，通过算法生成口令。G 节点和 T 节点基于该口令进行 SLB 关联。流程描述如下：

1. T 节点向 G 节点发送关联请求消息，携带 T 节点 ID、随机数 NONCEt。

2. G 节点生成随机数 NONCEg，根据密钥协商算法生成 Kgt。G 节点生成口令=KDF (G 节点 ID, T 节点 ID, NONCEt, NONCEg)，并根据口令生成 PSK，PSK=KDF（Kgt，口令, T 节点 ID, G 节点 ID, NONCEt, NONCEg）。G 节点生成认证参数 AUTHg=KDF(PSK，$K_{KE}$, NONCEg，关联请求消息)|高 32 比特。G 节点向 T 节点发送安全上下文请求消息，携带随机数 NONCEg 和 AUTHg。

3. T 节点根据密钥协商算法生成 Kgt。G 节点生成口令=KDF (G 节点 ID, T 节点 ID, NONCEt, NONCEg)，并根据口令生成 PSK，PSK=KDF（Kgt，口令, T 节点 ID, G 节点 ID, NONCEt,

NONCEg）。T 节点基于 PSK 验证 AUTHg 是否正确。如果 AUTHg 验证不通过，T 节点丢弃该消息。T 节点向 G 节点发送安全上下文响应消息。消息中携带认证参数 AUTHt。AUTHt = KDF (PSK, $K_{KE}$, 安全上下文请求消息, NONCEt, G 节点密钥协商算法能力)|高 32 位

4. G 节点验证 AUTHt。G 节点向 T 节点发送关联建立消息。

G 节点和 T 节点保存 PSK，以及 PSK 和对端 ID 的对应关系，后续直接使用该 PSK 进行 SLB 关联。

G 节点和 T 节点采用此种方法生成口令，可以加入限制条件，即满足限制条件才能使用该方法. 限制条件如：

- G 节点和 T 节点无对应于对端节点的 PSK
- G 节点和 T 节点互相交换自己的 IO 能力（输入输出能力），至少有一方为无输入无输出能力

# 第六章 总结与展望

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。

本解决方案白皮书重点梳理了星闪技术在智能汽车和智能终端领域在星闪网络安全标准落地时面临的业务需求，并基于这些需求提出了可参考的网络安全解决方案。

作为新一代无线短距通信技术，构建网络安全技术竞争力并推动产业的规模落地对星闪技术的实际商用至关重要。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. 加速推动星闪 Release 1.0 网络安全技术的产品落地和实际商用。推动网络安全解决方案、测试认证等环节，推动星闪网络安全技术在四大领域的高价值场景中率先实现规模商用。