An Authentication and Key Agreement Scheme for NearLink Wireless Networks in Industrial Systems*

WANG Yuling[1,2,3], JIN Xi[2,3*], XU Chi[2,3], XIA Changqing[2,3], SUN Yiming[2,3], DUAN Yong[1]
(1.School of Information Science and Engineering, Shenyang University of Technology, Shenyang Liaoning 110870, China;
2.Key Laboratory of Networked Control Systems, Chinese Academy of Sciences, Shenyang Liaoning 110016, China;
3.Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang Liaoning 110016, China)

Abstract: NearLink, a new generation communication network technology led by Huawei, is still in the early stages of development and the security strategy needs to be improved. A lightweight authentication and key negotiation scheme applicable to NearLink is proposed to meet the high security requirements of industrial systems. This scheme covers authentication and key negotiation between industrial nodes and central servers, as well as direct authentication and key negotiation between industrial nodes. By using physical unclonable functions, aggregated message authentication codes, and reusing key/session parameters generated during the authentication stage, it avoids multiple rounds of interaction between industrial nodes and central servers. The verification results of Scyther confirms that this scheme meets security capabilities such as bidirectional authentication, confidentiality protection, and resistance to protocol attacks. In comparison with similar schemes, this scheme not only ensures more comprehensive security, but also reduces about 30% of communication overhead and 98% of computational overhead, making it suitable for resource limited industrial NearLink devices.

Key words: communication network technology; security authentication; key agreement; Scyther formal verification; NearLink technology; industrial systems
EEACC: 6210Z **doi**: 10.3969/j.issn.1004-1699.2026.09.023

面向工业系统的星闪无线网络认证与密钥协商方案*

王玉玲[1,2,3], 金 曦[2,3*], 许 驰[2,3], 夏长清[2,3], 孙乙铭[2,3], 段 勇[1]
(1.沈阳工业大学信息科学与工程学院, 辽宁 沈阳 110870; 2.中国科学院网络化控制系统重点实验室, 辽宁 沈阳 110016; 3.中国科学院沈阳自动化研究所, 辽宁 沈阳 110016)

摘 要: 针对华为牵头制定的新一代通信网络技术——星闪, 正处于发展初期, 安全策略仍需完善这一问题, 提出了一种可应用于星闪的轻量级安全认证与密钥协商方案, 使星闪能够满足工业系统的高安全性需求。该方案涵盖了工业节点和中央服务器之间的认证与密钥协商, 以及工业节点之间直接的认证与密钥协商, 通过物理不可克隆函数、聚合消息认证码和复用认证阶段产生的密钥/会话参数, 避免了工业节点与中央服务器间的多轮交互。Scyther 的形式化验证证实了该方案能够满足双向认证、机密性保护和抗协议攻击等安全需求。在与同类方案的比较中, 该方案不仅保证了更全面的安全性, 还减少了约 30%的通信开销和 98%的计算开销, 可用于资源受限的工业星闪设备。

关键词: 通信网络技术; 安全认证; 密钥协商; Scyther 形式化验证; 星闪技术; 工业系统
中图分类号: TP393 **文献标识码**: A **文章编号**: 1004-1699(2026)09-2106-09

星闪技术[1]于 2020 年由华为牵头制定, 目的是弥补现有短距离无线通信技术(例如蓝牙、WiFi)的不足, 提出的一体化技术架构能够全面支撑传感、控制等多类型无线应用。同时, 该技术的提出使我国的短距离无线通信技术完全自主可控, 国内相关产品不受国外制裁。星闪网络的极低延时和高可靠特性使工业控制的无线化成为可能[2]。但是在工业场景中, 工业无线网络必须配备高安全性保障机制。星闪安全相关的标准[3]中规划了完整的安全架构, 但切实可用的安全方案并不在标准规划范围内, 且目前处于星闪商用初期, 各厂商和研究机构均未披露各自产品是否考虑了安全问题, 或者使用了何种

项目来源: 国家自然科学基金项目(62133014, 62173322, 92267108, 62303449); 中国科学院青促会项目(Y2021062, 2020207); 辽宁省科技计划(2023JH3/10200006, 2023JH3/10200004, 2022JH25/10100005, 2023-BS-029); 机器人学国家重点实验室自主课题(2024-Z12); 兴辽人才项目(XLYC2202048); 中国高校产学研创新基金项目(2025ZX012)
收稿日期: 2024-05-14 **修改日期**: 2024-10-09

安全方案。

星闪与蓝牙、WiFi 同属短距离通信技术。蓝牙技术中包含一种建立安全连接的安全简单配对(Simple Secure Pairing,SSP)技术。文献[4]分析了 SSP 协议在蓝牙基本速率/增强数据速率和低功耗蓝牙操作模式下的安全性。Kwon 等[5]通过应用密文策略属性的加密,提出了两种基于蓝牙配对的 D2D(Device-to-Device)安全密钥建立和认证协议。在 Wi-Fi 技术中,用于建立安全连接的主要方法是 WPA(Wi-Fi Protected Access)。文献[6]使用高效的基于身份的加密(Identity-Based Encryption,IBE)技术设计一种新的无线安全协议,用于隐私和身份验证。文献[7]针对 WPA2 身份认证协议存在的安全问题提出了一种基于椭圆曲线离散对数理论的身份认证协议改进方法。但已有的蓝牙和 WiFi 安全方案面向民用系统而设计,难以满足工业系统的高安全需求,相关的安全机制难以借鉴。与之相比,5G 的安全机制更为健全。5G 中的安全方案分为两类:传统安全方案和基于组的安全方案。在传统方案的研究中,Huang 等[8]提出了一种能够抵抗典型攻击的安全认证协议 SAKA。3GPP 委员会曾指出,每个窄带物联网设备都需要执行基本的 5G 身份认证和密钥协议(5G-AKA)流程或可扩展身份验证协议身份验证和密钥协议(EAPAKA')流程,以实现与 3GPP 核心网的相互认证[9]。然而以上协议缺乏群组认证机制,过程需要多轮信令交换,并且导致大量的信令开销和通信开销。在基于组的安全方案中,Cao 等[10]提出了一种轻量级安全接入认证方案 LSAA,该方案分别用于两种移动设备:普通用户设备(User Equipment,UE)和大规模机器类通信设备(massive Machine Type Communication,mMTC)设备,虽然系统开销较小,但无法抵御物理攻击。Li 等[11]提出了一种基于组的 AKA 协议 GRAKA,该协议通过使用秘密共享方案和 Diffie-Hellman(DH)密钥协商协议,同时在 MTC 设备组和 MME(Mobility Management Entity)之间实现相互认证。Lu 等[12]采用基于双线性对函数的批量验证技术,提出了一个高效且隐私保护的聚合方案。然而,5G 属于高性能系统,以上研究是用资源的高开销换取高安全性,而星闪采用嵌入式终端,资源有限,难以支撑 5G 的安全机制。

本文的研究在 5G 认证与密钥协商思想的基础上,设计了一种面向星闪的轻量级认证与密钥协商方案。该方案涵盖了工业节点和中央服务器之间的认证与密钥协商,以及工业节点之间直接的认证与密钥协商,通过物理不可克隆函数、聚合消息认证码和复用认证阶段产生的密钥/会话参数,避免了工业节点与中央服务器的多轮交互,减少了网络通信的复杂度和资源消耗,同时实现了轻量化。本文使用 Scyther 对所提方案进行形式化验证,验证结果证实了本方案能够满足双向认证、机密性保护和抗协议攻击等安全需求。在与同类方案的比较中,本方案不仅保证了更全面的安全性,还减少了约 30%的通信开销和 98%的计算开销,以少量资源实现了全网节点间的高安全性通信。

1　网络架构

星闪节点依据功能的不同分为管理节点(G 节点)和终端节点(T 节点)。G 节点与 T 节点之间可进行一对多的连接。以一个 G 节点为中心的星型拓扑网络称为一个域,如图 1 所示。当多个域需要协同时,G 节点可退化为 T 节点,从而实现多域的连接。

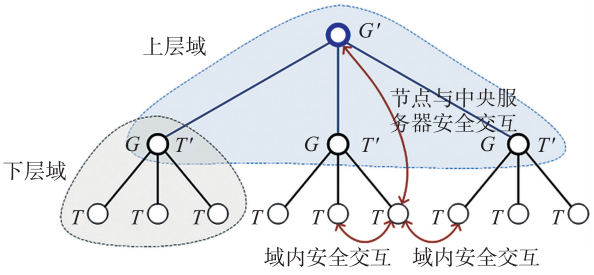


图 1　网络架构

工业系统中存在大量分布在物理空间的感知、控制、中继等具有无线传输能力的节点。由于数量过多,以及距离较远,这些节点无法在同一个域内进行管理,因此本文采用两层多域级联的方式对其进行组织。下层的 T 节点和 G 节点对应大量的工业节点,上层的 G' 节点是工业系统的中央服务器,配备了星闪无线模组,具有对所有节点进行安全性认证和密钥协商的功能。在工业场景中,当一个或多个节点移动到其他域时,则需要对新入网节点进行认证。目前星闪模组一跳距离为 219 m[13],随着技术的演进,未来一跳可达 1 km,所以两层网络可以覆盖大多数的厂区,即使面对更大规模的厂区,可以在 G' 与 G 之间增加中继节点进行透明转发,并不影响安全方案的执行。另外,网络节点的组网问题在无线传感网络中已有大量研究[14],本文不再设计相应的组网算法。工业节点组网后的网络结构作为本文研究内容的已知条件给出。

由于在工业系统中,不仅所有工业节点需与中央服务器进行交互,工业节点间也存在直接交互的

需求。例如,轧钢产线中板材速度异常时,感知节点会向中央服务器发报警信息,同时向监控节点发送命令,提升监控视频清晰度。因此本文所提出的认证与密钥协商方案不仅支持节点与中央服务器间的安全交互,还支持节点间的安全交互。

2 认证与密钥协商方案

基于星闪网络架构和安全交互需求,本文所提认证与密钥协商方案包括三个阶段:初始化阶段、全网节点与 G' 间的认证与密钥协商阶段、T 节点间的信任建立阶段。方案中相关符号如表 1 所示。

表 1 符号的定义

符号	定义
T_i	第 i 个设备节点
ID_i	T_i 的身份索引
PID_i	ID_i 的伪身份
GID	域身份
CRP	PUF 的挑战-响应对
C_i	节点 T_i 的 PUF 挑战
R_i	C_i 的响应
r_i	T_i 产生的随机数
$r_{G'}$	G'产生的随机数
$H_i(i=1,\cdots,6)$	$H_i:\{0,1\}^*\rightarrow\{0,1\}^k$
K_i	共享密钥
GK	域密钥
SK_i	T_i 的会话密钥
MAC	消息认证码
G_1,G_2	第 1 个域、第 2 个域
m	域的数量
n	T_i 的数量
$\mathrm{TAG}_1,\mathrm{TAG}_2$	域内和域外广播标识
bid	广播的随机索引号

2.1 初始化阶段

节点 T_i 具有真实身份 ID_i 及自身所在域的标识 GID,且支持 PUF(Physical Unclonable Function)。PUF 是一种利用电子器件物理特性产生唯一响应的安全技术,在文献[15]中首次被提出。其核心思想是:由于制造过程中的微小差异,即便是使用相同设计和工艺制造的集成电路,也会拥有独特的、不可预测的物理特性。PUF 被表示为函数 P,$R=P(C)$,其中 C 和 R 分别是 PUF 的输入挑战和输出响应,由此每个节点生成挑战-响应对 CRP(C_i,R_i)。管理节点 G 可退化为 T_i 节点,且参与域内的消息聚合,因此同样具有自己的真实身份 ID_G 及域标识 GID。当初始化阶段完成后,节点 T_i 中存储了真实身份 ID_i、域标识 GID 以及初始 CRP 的挑战 C_i,服务器 G' 端存储每个节点 T_i 的真实身份 ID_i、初始 CRP、管理节点 G 的身份 ID_G、各域标识 GID 以及自身的身份 $\mathrm{ID}_{G'}$。

2.2 全网节点与 G'间的认证与密钥协商阶段

在该阶段,中央服务器节点 G'对接入网络的节点进行认证,并且在 G'和每个节点 T_i 之间创建一个独有的会话密钥。此过程不仅确保了节点的合法性和会话的安全性,而且为域内节点之间,以及同一网络环境下不同域节点间后续的认证活动提供了必要的信息。其流程如图 2 所示。

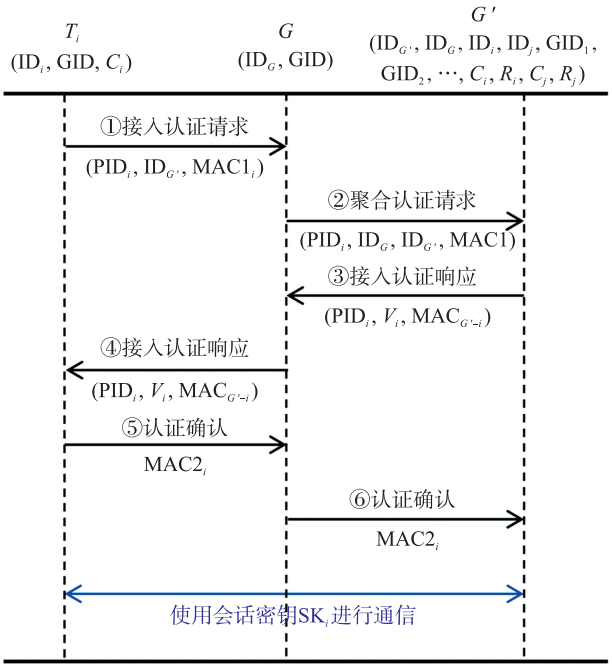


图 2 全网节点与 G′间的认证与密钥协商流程图

具体描述如下:

①$T_i\rightarrow G$:节点 T_i 生成随机数 r_i,并将挑战 C_i 基于 $R=P(C)$ 生成的响应值 R_i 与 r_i 结合,计算其初始假名 $\mathrm{PID}_i=H_1(\mathrm{ID}_i,P(C_i))\oplus r_i$,然后将其假名 PID_i、所在域的标识 GID、随机数 r_i 以及计划接入的网络 $\mathrm{ID}_{G'}$作为生成消息认证码 $\mathrm{MAC1}_i$ 的输入,即计算 $\mathrm{MAC1}_i=H_6(\mathrm{PID}_i,\mathrm{GID}_1,r_i,\mathrm{ID}_{G'})$,最后将认证请求信息($\mathrm{PID}_i$,$\mathrm{ID}_{G'}$,$\mathrm{MAC1}_i$)发送给所在域的管理节点 G。

②$G\rightarrow G'$:管理节点 G 接收到域内所有节点发来的认证请求信息后,将所有节点的消息认证码 $\mathrm{MAC1}_i$ 进行聚合,生成聚合消息认证码 $\mathrm{MAC1}=\mathrm{MAC1}_1\oplus\mathrm{MAC1}_2\oplus\cdots\oplus\mathrm{MAC1}_n$,接着将信息($\mathrm{PID}_i$,$\mathrm{ID}_G$,$\mathrm{ID}_{G'}$,MAC1)发送给中央服务器节点 G'进行认证。相比每个节点单独发送认证码,这种方法显著减少了通信次数和传输的数据量,从而减轻了网络负担,实现了通信层面的轻量化。

③$G'\rightarrow G$:G'端首先验证所收到的信息中的 $\mathrm{ID}_{G'}$ 与自身网络身份信息是否匹配,不匹配则终止验证;

若匹配,则继续验证该信息中管理节点的 ID_G。基于存储信息判断 ID_G 是否为自身网络下的管理节点 G,若不是则同样终止验证;若为合法管理节点 G,则进行后续步骤。G'通过已存储信息,基于 ID_G 检索出域标识 GID 以及对应域节点的$\{ID_i, C_i, R_i\}$,根据检索信息计算出随机数 $r_i = PID_i \oplus H_1(ID_i, R_i)$,进而验证 MAC1,验证成功后 G'生成随机数 $r_{G'}$,计算 $V_i = H_3(PID_i, ID_{G'}) \oplus r_{G'}$来隐藏随机数,同时生成共享密钥 $K_i = H_2(r_{G'}, PID_i)$、会话密钥 $SK_i = H_4(PID_i, GID_1, K_i, r_i)$、域密钥 $GK = H_5(r_{G'}, GID_1)$以及消息认证码 $MAC_{G'-i} = H_6(PID_i, GID_1, ID_{G'}, V_i, K_i, GK, r_{G'}, r_i)$,最后 G'将认证响应消息$(PID_i, V_i, MAC_{G'-i})$发送给管理节点 G。

④$G \rightarrow T$:管理节点 G 广播认证响应消息$(PID_i, V_i, MAC_{G'-i})$。

⑤$T \rightarrow G$:所有节点 T_i 通过广播消息中的 PID_i 来接收对应信息$(V_i, MAC_{G'-i})$,然后计算 $r_{G'} = V_i \oplus H_3(PID_i, ID_{G'})$,根据得出的 $r_{G'}$ 计算 K_i、GK,进而验证 $MAC_{G'-i}$,若成立,则继续生成$(MAC2_i, MACI_i^{G1}, MACE_i^{G1})$,并将确认信息 $MAC2_i = H_6(PID_i, GID_1, ID_{G'}, K_i, GK, SK_i)$发送给管理节点 G。其中 $MACI_i^{G1}$ 和 $MACE_i^{G1}$ 分别用于后续的同域节点间的认证和不同域节点间的认证。

⑥$G \rightarrow G'$:同样地,管理节点 G 接收到域内所有节点发来的确认消息后,将每个节点 T_i 的消息认证码 $MAC2_i$ 进行聚合,生成聚合消息认证码 $MAC2 = MAC2_1 \oplus MAC2_2 \oplus \cdots \oplus MAC2_n$,接着将聚合信息 MAC2 发送给 G'。G'在接收到消息后根据已有信息计算 $MAC2_i$ 进而验证 MAC2,若成立则确认所有节点成员有效,否则不足以进行认证。

2.3　T 间的信任建立阶段

基于上述已有的网络认证基础,属于同一网络的各域节点 T_i 均已完成身份验证,并且获得了相应的共享密钥 K_i、域密钥 GK、会话密钥 SK_i。其中 SK_i 用于确保节点与网络之间后续交互的安全通信,而域密钥 GK、共享密钥 K_i 分别用于完成同域节点以及不同域节点间的认证,无需再次与网络交互获得相关密钥参数,进而减少通信开销。在全网节点与 G'间的认证与密钥协商阶段的步骤⑤中描述道,$MACI_i^{G1}$ 和 $MACE_i^{G1}$ 分别用于后续的同域节点间的相互认证和不同域节点间的直接认证,其中 $MACI_i^{G1} = H_6(bid_1, PID_i^{G1}, GID_1, K_i^{G1}, GK)$,以及 $MACE_i^{G1} = H_6(bid_3, PID_i^{G1}, GID_1, ID_{G'}, K_i^{G1})$。基于此,$T$ 间的信任建立流程如图 3 所示。

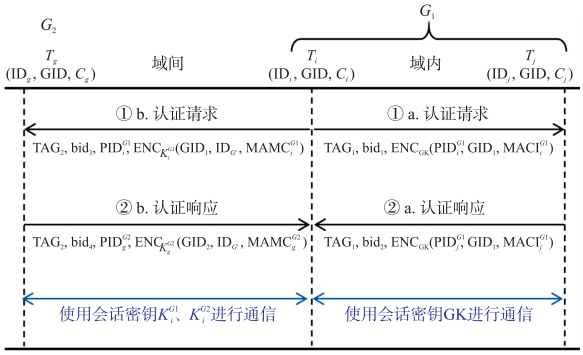


图 3　T 间的信任建立流程

具体如下:

①节点 T_i 广播消息。对于域 1(G_1)的节点 T_i,向同域其他所有节点广播消息$\{TAG_1, bid_1, ENC_{GK}(PID_i^{G1}, GID_1, MACI_i^{G1})\}$,即将节点 T_i 的相关信息 PID_i^{G1}、GID_1、$MACI_i^{G1}$ 用域密钥 GK 进行加密传送。同时向网络 G'下的其他域节点广播消息$\{TAG_2, bid_3, PID_i^{G1}, ENC_{K_i^{G1}}(GID_1, ID_{G'}, MACE_i^{G1})\}$,即将信息 GID_1、$ID_{G'}$、$MACE_i^{G1}$ 用共享密钥 K_i^{G1} 进行加密传送,其中 TAG_1 代表域内广播标志,TAG_2 代表域外广播标志,bid 代表广播的随机索引号。

②其余节点对 T_i 的认证及密钥协商。

A. 同域的其他节点 T_j 在监听到标志为 TAG_1 的广播消息后,用域密钥 GK 对密文进行解密获得节点 T_i 的 PID_i^{G1}、GID_1、$MACI_i^{G1}$,在通过 GID_1 证明是同域的节点后,计算 $K_i^{G1} = H_2(r_{G'}, PID_i^{G1})$,进而验证 $MACI_i^{G1}$,若验证成功则代表 G_1 内的节点 T_j 成功认证节点 T_i。节点 T_j 接着生成 $MAC_j^{G1} = H_6(bid_2, PID_j^{G1}, GID_1, K_j^{G1}, GK)$,同理向同域其他节点发送广播消息$\{TAG_1, bid_2, ENC_{GK}(PID_j^{G1}, GID_1, MACI_j^{G1})\}$。

B. 域 2(G_2)的节点 T_g 在监听到标志为 TAG_2 的广播消息后,计算 $K_i^{G1} = H_2(r_{G'}, PID_i^{G1})$,用共享密钥 K_i^{G1} 对密文进行解密获得 G_1 节点的相关信息 GID_1、$ID_{G'}$、$MACE_i^{G1}$,在验证 GID_1、$ID_{G'}$成功后(即证明该 GID_1 域节点与自己同处相同网络 $ID_{G'}$下),进而验证 $MACE_i^{G1}$,若验证成功则代表的 G_2 节点 T_g 成功认证 G_1 的节点 T_i。G_2 节点接着生成 $MACE_g^{G2} = H_6(bid_4, PID_g^{G2}, GID_2, ID_{G'}, K_g^{G2})$,向 G_1 发送广播消息$\{TAG_2, bid_4, PID_g^{G2}, ENC_{K_g^{G2}}(GID_2, ID_{G'}, MACE_g^{G2})\}$。

③T_i 对其余节点的认证及密钥确认。

A. G_1 的节点 T_i 监听到标志为 TAG_1 的同域节点 T_j 的广播消息,用域密钥 GK 对密文进行解密获得节点 T_j 的 PID_j^{G1}、GID_1、$MACI_j^{G1}$,在通过 GID_1 证明

是同域的节点后，计算 $K_j^{G1}=H_2(r_{G'},\mathrm{PID}_j^{G1})$，进而验证 MACI_j^{G1}，验证成功则节点 T_i 成功认证节点 T_j，即实现了 G_1 节点 T_i 与 T_j 的相互认证，后续通过域密钥 GK 进行安全通信。

B. G_1 的节点监听到标志为 TAG_2 的广播消息后，计算 $K_g^{G2}=H_2(r_{G'},\mathrm{PID}_g^{G2})$，用共享密钥 K_g^{G2} 对密文进行解密获得 G_2 节点的相关信息 GID_2、$\mathrm{ID}_{G'}$、MACE_g^{G2}，在验证 GID_2、$\mathrm{ID}_{G'}$ 成功后，进而验证 MACE_g^{G2}，验证成功则 G_1 和 G_2 的节点完成相互认证，后续通过共享密钥 K_i^{G1}、K_g^{G2} 进行安全通信。

3 安全性评估

3.1 Scyther 形式化验证

本文使用了形式化验证工具 Scyther[16] 对提出的方案进行验证。采用 Scyther2 版本的 Compromise-0.9.2，并选择 Dolev-Yao 作为本文方案的安全模型，将 T 和 G′设置为两个实体来简化协议的描述。从图 4 可以看出，所提出的方案满足设置的所有 claim 事件，并且没有产生攻击，因此，所提协议满足了所选安全模型中的安全要求。

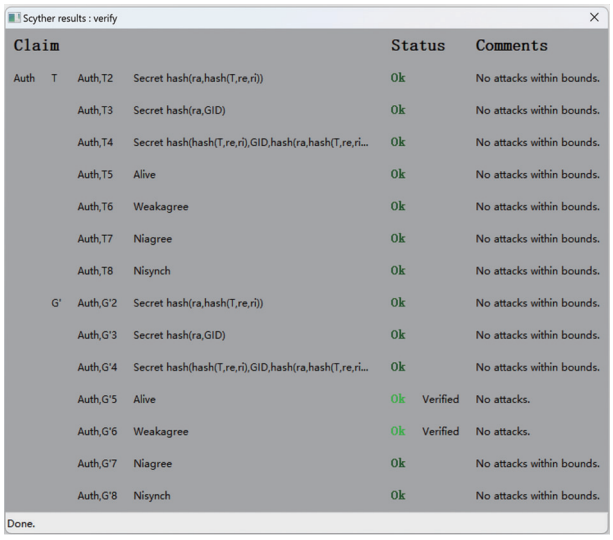


图 4 Scyther 验证结果

3.2 安全性分析

本文所提方案具有以下安全属性：

①相互认证和密钥协商：一方面 G' 通过验证 $\mathrm{MAC1}_i$ 来认证节点 T，由于响应值 R_i 以及节点产生的随机数 r_i 只在 T 与 G' 之间共享，一旦出现无效的节点 T，验证就会失败。另一方面，T 通过验证 $\mathrm{MAC}_{G'-i}$ 来认证 G'，因为只有经过认证的 G' 才能得到 PID_i 和相应的秘密参数，从而实现了 T 与 G' 之间的相互认证。此外，通过 R_i、r_i 计算出的 PID_i 同样在 T 与 G' 之间共享，G' 通过自身生成的随机数 $r_{G'}$ 可以安全获得 K_i，T 也可通过计算获得 $r_{G'}$、K_i，因此 T 与 G' 建立了相互秘密参数和相同的会话密钥。

②匿名性：节点 T 在认证请求及响应过程中均采用假名 PID_i 而不是真实身份 ID_i 来标识节点，并且 PID_i 是通过 R_i、r_i 计算而出，任何敌手都无法从 PID_i 获得 ID_i。

③不可追踪性：与同一节点 T 最直接关联的信息只有伪身份 PID_i，而所提方案在每次认证成功后，PID_i 会通过随机数 r_i 进行更新，保证了每一认证周期中 PID_i 的唯一性与不可预测性，由于敌手缺乏对随机数 r_i 及更新机制的了解，无法将不同认证轮次中的 PID_i 关联至同一节点 T。

④不可链接性：由于 T 端生成的随机数 r_i 和 G' 端生成的随机数 $r_{G'}$ 使得每个会话中都采用了随机数，无法确认来自同一用户的多次会话是否源自同一用户。

⑤前向/后向保密性：会话密钥 SK_i 的生成涉及到随机数的参与，这一设计确保了即便攻击者成功获取了某些会话密钥，也无法利用这些信息推算出其他会话期间使用的密钥。

⑥密钥确认：本方案在 T 成功验证 $\mathrm{MAC}_{G'-i}$ 后完成了与 G' 之间的相互认证，而后发送的密钥确认信息 $\mathrm{MAC2}_i$ 在被 G' 成功验证后，认证双方均确认密钥已被对方正确获得，确保了密钥交换过程中的双向验证。

⑦抗协议攻击：由于使用了随机数 r_i、$r_{G'}$，当来自 T 的认证请求消息和来自 G' 的认证响应消息被重放时，双方可以检查消息认证码来抵抗重放攻击。会话密钥 SK_i 的生成基于 T 和 G' 内预先存储的机密数据以及 PUF 产生的 CRP 对，这一过程不依赖于公共信道的数据传输，而且实现了 T 与 G' 之间的相互认证与密钥协商，因此可以抵抗中间人攻击。此外，每个域成员无法获得彼此的 R_i 和 K_i 来计算各自的消息认证码，因此可以抵抗伪造攻击。

⑧抗物理和克隆攻击：节点 T 无需存储任何机密数据，而且方案中采用 PUF 技术，通过在 T 与 G' 间交换 PUF 挑战和响应值，确保了双方通信的安全性。得益于 PUF 的固有特性，即其响应的唯一性和不可预测性，本方案能有效防御物理攻击及克隆攻击。

针对上述安全属性，相关协议的比较如表 2 所示，其中 NLAKA 为本文所提方案的简称。可以看到，本方案具有更全面的安全性。

表 2　所有方案的安全性比较

安全属性	MTCAKA[17]	SEAKA[18]	EGAKA[19]	LPPA[20]	GBAAM[21]	LGTH[22]	NLAKA
相互认证和密钥协商	√	√	√	√	√	√	√
匿名性	×	√	√	√	×	×	√
不可追踪性	×	×	×	×	×	×	√
不可链接性	×	×	×	×	×	×	√
前向/后向保密性	×	√	√	×	√	×	√
密钥确认	×	×	×	×	×	×	√
抵抗重放攻击	√	√	×	×	√	×	√
抵抗中间人攻击	√	√	√	√	√	√	√
抵抗伪造攻击	√	√	√	√	√	×	√
抵抗物理和克隆攻击	×	×	×	×	×	×	√

4　性能比较

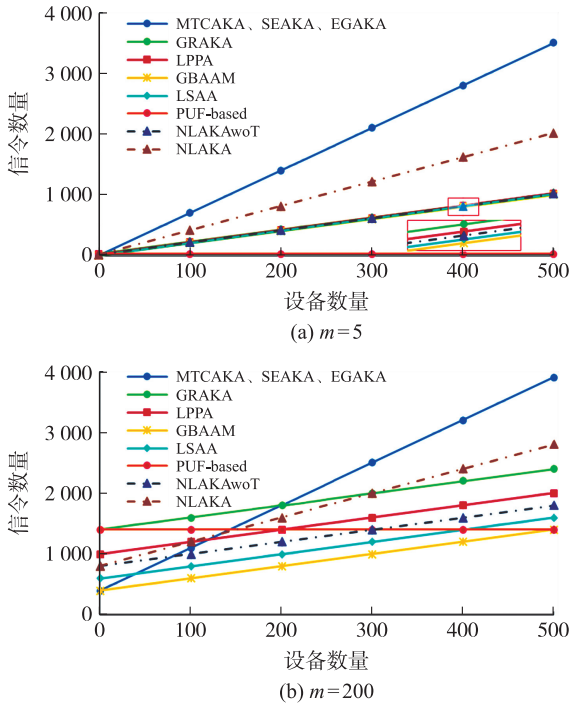
本节将比较所提方案与其他相关方案的信令开销、通信开销和计算开销。由于本文所提方案集成了 T 与 G'间的认证以及 T 间的相互认证,为更准确地与相关方案进行比较,本方案的整体过程为 NLAKA,仅 T 与 G'间的过程表示为 NLAKAwoT。

4.1　信令开销比较

本研究中的管理节点 G 等同于相关方案中的组长节点,相关方案用于比较的信令开销来自于文献[23],表 3 为本文比较的全部信令开销。图 5 所示为 $m=5$ 和 $m=200$ 时的多种方案信令开销随节点数量变化的结果比较。对比方法 MTCAKA、SEAKA、EGAKA、GRAKA 和 LPPA 的信令开销多于本文方案。对比方法 LSAA、GBAAM 和部分 PUF-Based 的信令开销虽然小于本文方案,但 NLAKA 包含了 T 间的认证与密钥协商流程,以及 NLAKAwoT 包含 T 间流程所需要的基础参数,所以虽然 LSAA、GBAAM 和 PUF-Based 具有更少的信令开销,但无法实现 NLAKA 和 NLAKAwoT 对 T 间流程的支持。在不支持 T 间认证和密钥协商的方案中,T 间数据交互只能通过管理节点或中央服务器进行转发,最终导致数据交互的开销至少增加 1 倍。

表 3　信令开销比较

方案	信令开销
MTCAKA[17]、SEAKA[18]、EGAKA[19]	$7n+2m$
GRAKA[11]	$2n+7m$
LPPA[20]	$2n+5m$
GBAAM[21]	$2n+2m$
LSAA[10]	$2n+3m$
PUF-Based[23]	$7m$
NLAKAwoT	$2n+4m$
NLAKA	$4n+4m$



(a) $m=5$

(b) $m=200$

图 5　多种方案的信令开销比较

4.2　通信开销比较

表 4 给出了本文所提方案中相关参数的通信开销,其中挑战值 C 及响应值 R 均设为 128 比特,随机数 r_i、$r_{G'}$设置为 64 比特,ID、PID 和 GID 的大小同样设为 128 比特。本方案采用的安全哈希算法的输出结果为 128 比特。表 5 所示为本方案与对比方案的通信开销。

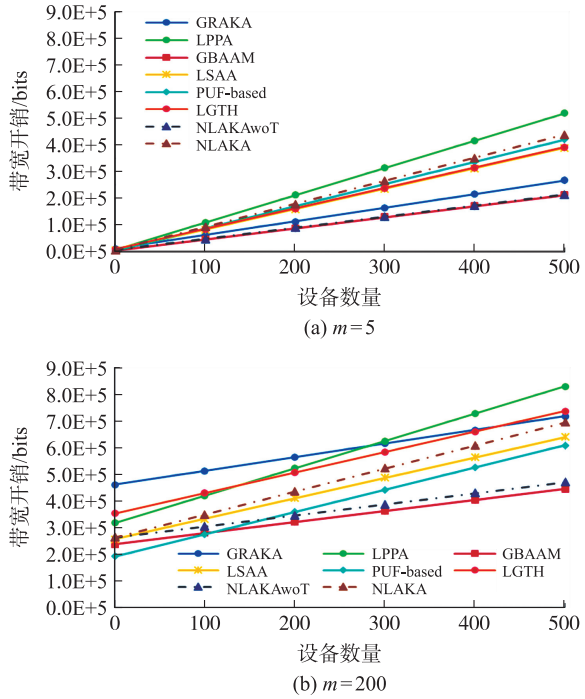
表 4　参数长度

参数	大小/bits
C	128
R	128
r_i、$r_{G'}$	64
ID、PID、GID	128
$H(\cdot)$	128

表 5 通信开销比较

方案	通信开销
GRAKA[11]	512n+2 304m
LPPA[20]	1 024n+1 584m
GBAAM[21]	416n+1184m
LSAA[10]	768n+1 280m
PUF-Based[22]	832n+960m
LGTH[23]	768n+1 760m
NLAKAwoT	416n+1 312m
NLAKA	448n+416n+1 312m

由于节点与服务器之间交互产生的密钥/会话参数,为后续节点间交互认证提供了基础,使得节点间的认证过程无需再与服务器端多次交互,从而减少了数据包的传递次数、减少了通信开销。当 $m=5$ 和 $m=200$ 时,多种方案通信开销随节点数量变化的比较结果如图 6 所示。NLAKA 的通信开销为 864n+1 312m,其中有 448n 是 T 间流程的开销,NLAKAwoT 部分的开销是 416n+1 312m。由比较结果可知,本文所提方案具有较小的通信开销,仅 GBAAM 的通信开销比本文所提方法少约 7%,但 GBAAM 无法支持后续的 T 间流程,不适用于星闪网络架构下的认证与密钥协商。与通信开销最大的 LPPA 相比,NLAKA 只使用了不到其通信资源的 70%,减少了约 30%的通信开销,实现了更全面的安全防护。



(a) $m=5$

(b) $m=200$

图 6 多种方案的通信开销比较

4.3 计算开销比较

计算开销基于图 7 所示的实验平台获得,其中星闪模组采用 Lierda 的 EB25[13],T 节点和管理节点基于树莓派 4B 实现,中央服务器采用配置为 i5 2.5 GG 处理器+16 GB 内存的笔记本电脑实现,计算相关的软件程序包为 OpenJDK-18.0.2.1、jPBC-2.0.0 和 bcprov-jdk16-1.46。计算开销用关键运算的执行时间衡量,关键运算如表 6 所示,包括哈希运算时间 T_h,点乘运算时间 T_m,对称加密/解密运算时间 T_e,PUF 运算时间 T_{PUF},配对运算时间 T_p。本文所提方案 NLAKA 和对比算法的计算开销如表 7 所示。

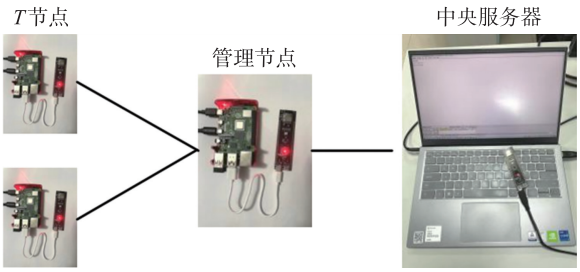


图 7 实验平台

表 6 关键运算的执行时间

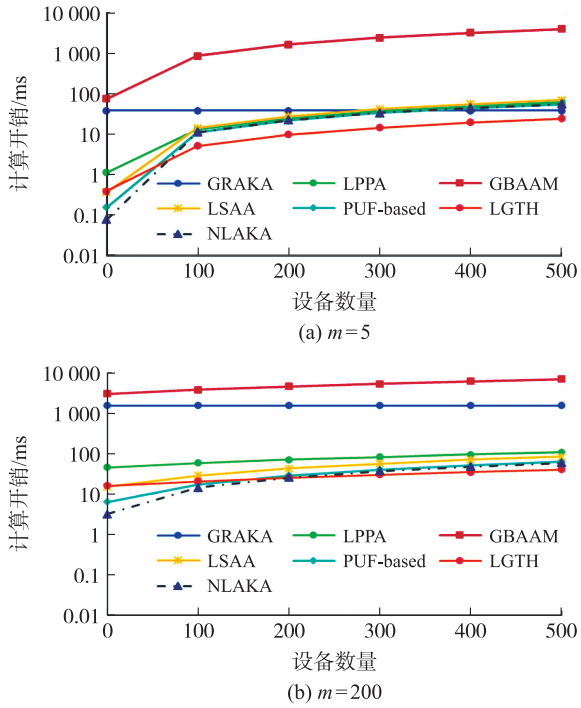
参数	消耗时间/ms
T_h	0.016
T_m	3.87
T_e	0.059
T_{PUF}	0.079
T_p	3.67

表 7 计算开销比较

方案	设备	管理节点	中央服务器
GRAKA[11]	$2T_m+T_h$	$4T_h$	$2\ mT_m+3\ mT_h$
LPPA[20]	$2T_e+9T_h$	T_h+T_e	$(n+2m)T_e+(4n+7m)T_h$
GBAAM[21]	$6T_m+2T_h$	0	$(2n+2m)T_m+2nT_h+2\ mT_p$
LSAA[10]	$4T_h+2T_e$	T_e	$(n+m)T_e+(5n+m)T_h$
PUF-Based[22]	$8T_h+T_{PUF}$	T_h+T_{PUF}	$(7n+2m)T_h$
LGTH[23]	$6T_h$	0	$(3n+5m)T_h$
NLAKA	$(T_e+4T_h+)8T_h+T_{PUF}$	0	$(7n+m)T_h$

与其他方案相比,本文没有采用复杂的点乘及配对等需要长时间的运算,同时由于前文讲述的所节省的交互过程也减少了计算步骤,从而减少了计算开销。当 $m=5$ 和 $m=200$ 时,多种方案的计算开销随节点数量变化的比较结果如图 8 所示。NLAKA 的计算开销少于大部分对比方案的计算开销。仅部分 LGTH 以及节点数较多但域较少时的 GRAKA 具有更少的计算开销,但由表 2 可知,LGTH 和 GRAKA 的安全性极弱,所以计算开销少。与计算开销最大的 GBAAM 相比,NLAKA 仅用了其计算资源的 2%,减少了 98%的计算开销,支撑了更多了

安全属性。因此,NLAKA 以较小的计算开销换取了高安全性。



(a) $m=5$

(b) $m=200$

图 8　多种方案的计算开销比较

5　结论

星闪技术作为一种国内具有自主知识产权的新兴无线技术,在工业控制领域具有巨大的应用前景。本文通过对星闪技术的整理和分析,发现其低延时、高性能的特点能够满足工业系统对无线通信的严苛需求。为此,本文针对星闪技术设计了一种轻量级认证与密钥协商方案,以保证通信的安全性,同时尽可能减少系统资源的开销。通过对该方案的形式化验证和性能评估,验证了其在安全性和效率方面的可行性。然而,针对工业场景中的可移动节点,虽然仍可采用本方案,但需要针对移动性进行进一步的优化。未来工作也将集中在优化移动性节点的认证过程,同时进而优化认证协议,以适应更加复杂多变的工业应用场景。

参考文献:

[1] 国际星闪联盟. T/XS 00001-2022 星闪无线通信系统架构[S]. 深圳:国际星闪聪明,2022. http://sparklink.org.cn/standard/view.php? id=4.

[2] 智次方星闪 1.0 标准正式发布[EB/OL]. (2022-11-01)[2024-04-29]. https://www.thepaper.cn/newsDetail_forward_20618571.

[3] 国际星闪联盟. T/XS 40001-2022 星闪无线通信系统网络安全 通用要求[S]. 深圳:国际星闪聪明,2022. http://sparklink.org.cn/standard/view.php? id=12.

[4] Phan R C W, Mingard P. Analyzing the Secure Simple Pairing in Bluetooth v4. 0[J]. Wireless Personal Communications, 2012, 64(4): 719-737.

[5] Kwon H, Hahn C, Kim D, et al. Secure Device-to-Device Authentication in Mobile Multi-Hop Networks[C]//9th International Conference on Wireless Algorithms, Systems, and Applications, Harbin, China, 2014: 267-278.

[6] Mulkey C, Kar D C. Identity-Based Encryption Protocol for Privacy and Authentication in Wireless Networks[M]//Network Security Technologies: Design and Applications, Hershey, PA, USA, IGI Global, 2014: 129-155.

[7] 李晔桃. WPA2 身份认证协议安全研究与改进[D]. 西安:西安电子科技大学,2021.

[8] Huang Y L, Shen C Y, Shieh S W. S-AKA: A Provable and Secure Authentication Key Agreement Protocol for UMTS Networks[J]. IEEE Transactions on Vehicular Technology, 2011, 60(9): 4509-4519.

[9] 3rd Generation Partnership Project. System Architecture for the 5G System(3GPP TS 23.501 V16.7.0)[EB/OL]. Sophia Antipolis, France, 2021 (2021-01-12). https://portal. etsi. org/webapp/workprogram/Report _ WorkItem. app? WKI_ID=62182.

[10] Cao J, Yan Z, Ma R, et al. LSAA: A Lightweight and Secure Access Authentication Scheme for both UE and mMTC Devices in 5G Networks[J]. IEEE Internet of Things Journal, 2020, 7(6): 5329-5344.

[11] Li J, Wen M, Zhang T. Group-Based Authentication and Key Agreement with Dynamic Policy Updating for MTC in LTE-A Networks[J]. IEEE Internet of Things Journal, 2015, 3(3): 408-417.

[12] Lu R, Liang X, Li X, et al. EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(9): 1621-1631.

[13] 利尔达科技. Lierda EB25 模组通信拉距测试报告[R]. 杭州:利尔达科技,2023.

[14] Wohwe Sambo D, Yenke B O, Förster A. Optimized Clustering Algorithms for Large Wireless Sensor Networks: A Review[J]. Sensors, 2019, 19(2): 322.

[15] Pappu R, Recht B, Taylor J, et al. Physical One-Way Functions[J]. Science, 2002, 297(5589): 2026-2030.

[16] Cremers C J F. The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols[C]//20th International Conference on Computer Aided Verification, Princeton, NJ, USA, 2008: 414-418.

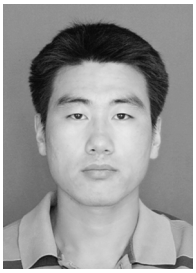
[17] Lai C, Li H, Li X, et al. A Novel Group Access Authentication and Key Agreement Protocol for Machine-Type Communication[J]. Transactions on Emerging Telecom-

munications Technologies,2015,26(3):414-431.
[18] Lai C,Li H,Lu R,et al. SE-AKA:A Secure and Efficient Group Authentication and Key Agreement Protocol for LTE Networks[J]. Computer Networks,2013,57(17):3492-3510.
[19] Jiang R,Lai C,Luo J,et al. EAP-Based Group Authentication and Key Agreement Protocol for Machine-Type Communications[J]. International Journal of Distributed Sensor Networks,2013,9(11):304601.
[20] Cao J, Ma M, Li H. LPPA: Lightweight Privacy-Preservation Access Authentication Scheme for Massive Devices in Fifth Generation(5G) Cellular Networks[J]. International Journal of Communication Systems,2019,32(3):e3860.
[21] Cao J, Ma M, Li H. GBAAM: Group-Based Access Authentication for MTC in LTE Networks[J]. Security and Communication Networks,2015,8(17):3282-3299.
[22] Lai C Z,Li H,Lu R X,et al. LGTH:A Lightweight Group Authentication Protocol for Machine-Type Communication in LTE Networks[C]//2013 IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, USA, 2013:832-837.
[23] Ren X,Cao J,Ma M,et al. A Novel PUF-Based Group Authentication and Data Transmission Scheme for NB-IoT in 3GPP 5G Networks[J]. IEEE Internet of Things Journal,2022,9(5):3642-3656.

王玉玲(2000—),女,现于沈阳工业大学信息科学与工程学院攻读硕士学位,中国科学院沈阳自动化研究所进行联培。主要研究方向为信息安全、网络性能优化,wangyuling@sia.cn;

金 曦(1983—),女,中国科学院沈阳自动化研究所研究员、博士。主要研究方向为网络安全、工业信息物理系统,xijin@ieee.org;

许 驰(1987—),男,中国科学院沈阳自动化研究所研究员、博士。主要研究方向为工业控制网络、工业无线网络,xuchi@sia.cn;



夏长清(1985—),男,中国科学院沈阳自动化研究所副研究员、博士。主要研究方向为网算协同、工业信息物理系统,xuchi@sia.cn;

孙乙铭(1992—),男,中国科学院沈阳自动化研究所副研究员、博士。主要研究方向为网络化控制系统设计,sunyiming@sia.cn;

段 勇(1978—),男,沈阳工业大学信息科学与工程学院教授、博士。主要研究方向为机器学习,计算机视觉,duanyong0607@sut.edu.cn。