基于异或自反性与射频指纹的无线组播密钥生成方法

开根深[1], 马俊韬[2], 武　刚[2], 胡　苏[2]

[1] 电子科技大学 信息与通信工程学院 成都 中国 611731
[2] 电子科技大学 通信抗干扰全国重点实验室 成都 中国 611731

摘要　随着物联网技术的发展, 组播通信的需求日益增大。异或加密作为最简单高效的加密方法之一, 在信息安全方面有着广泛的应用。本文针对组播通信安全需求, 设计了一种基于异或自反性和射频指纹的组密钥生成方法。为解决多个终端在密钥生成过程中的传输资源选择冲突问题, 提出基于扩频和公私钥密码体系的用户标识方法。先利用射频指纹对用户认证, 并在组播用户间形成密钥随机源; 然后, 利用异或的自反特性实现分布式密钥生成。将射频指纹与公私钥密码体系结合, 不仅为射频指纹的识别结果提供了参考, 还为组播通信下密钥协商时的通信资源选择提供了方法。为评估射频指纹识别的影响, 提出并实验验证了一种基于时频分析与深度学习的射频指纹识别算法。最后, 分析了所提方法的密钥生成率、资源选择冲突和密钥生成效率, 展示了所提方法的可行性和有效性。分析发现所提方法相比于传统方法, 分布式的密钥源使得密钥生成效率随着节点数的增大而提高。对组密钥被攻破概率的窃听模型仿真结果表明, 在生成同样长度的密钥时, 与遍历搜索密钥空间比较, 基于窃听者遍历搜索设备射频指纹特性的条件, 破解所提方法组密钥的复杂度要高出一至四个数量级, 验证了本文方法的安全性。

关键词　组密钥生成; 扩频技术; 射频指纹; 异或的自反性
中图法分类号　TN918　DOI 号 10.19363/J.cnki.cn10-1380/tn.2024.05.03

Group Key Generation Method Based on XOR Reflexivity and Radio Frequency Fingerprinting

KAI Genshen[1], MA Juntao[2], WU Gang[2] , HU Su[2]

[1] School of Communication & Information Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
[2] National Key Laboratory of Wireless Communications, University of Electronic Science and Technology of China, Chengdu 611731, China

Abstract　With the development of Internet of Things (IoT), there is an increasing demand for multicast communication. As one of the simplest and most efficient encryption methods, XOR encryption has a wide range of applications in information security. Aiming at the security requirements of multicast communication, this paper designs a group key generation method based on XOR reflexivity and radio frequency fingerprinting (RFF). In order to solve the conflict of transmission resource selection of multiple terminals in the process of key generation, this paper proposes a terminal identification method based on spread spectrum technology and public-private key cryptosystem. RFF are used to authenticate terminals, and a random source of keys is formed among multicast users. The purpose of distributed key generation is achieved by using the XOR reflexivity. By combining the RFF with the public-private key cryptosystem, it not only provides a reference for the identification results of the RFF, but also provides a method for the selection of communication resources during key negotiation under multicast communication. To evaluate the impact of RFF, a RFF recognition algorithm based on time-frequency analysis and deep learning is proposed and experimentally verified. Finally, the key generation rate, resource selection conflict and key generation efficiency of the proposed method are analyzed to illustrate the feasibility and effectiveness of the proposed method. The analysis reveals that the proposed method has a distributed key source compared to the traditional method, which makes the key generation efficiency increase as the number of nodes increases. The simulation results of the eavesdropping model of the probability of group key being breached show that, when generating a key of the same length, compared with traversing the search key space, based on the condition of the eavesdropper traversing the search device's RFF, the complexity of cracking the group key is one to four orders of magnitude higher, which verifies the security of the method in this paper.

Key words　group key generation; spread spectrum technology; radio frequency fingerprinting; XOR reflexivity

通讯作者：武刚, 博士, 教授, Email: wugang99@uestc.edu.cn。
本课题得到中央高校基本科研业务费专项资金(No. ZYGX2020ZB042)资助。
收稿日期: 2022-06-06; 修改日期: 2022-07-18; 定稿日期: 2024-01-18

1 引言

1.1 研究动机与背景

目前, 组播通信使用的通信安全方案是基于计算安全的、分发式的加密认证体系[1-3]。随着硬件算力的提升, 特别是量子计算技术的发展, 基于计算安全的加密体系的安全性越来越受到挑战。此外, 密钥的分发需要可信的第三方设备, 传统蜂窝移动通信中通常由鉴权中心完成这一任务, 而物联网组播场景中可信第三方部署是一个挑战。因此, 区块链与物联网的结合也受到较多关注, 例如文献[4]中指出可以将区块链技术与物联网集成设计安全认证与攻击防御机制。更重要的是, 依赖复杂对数计算执行加密/认证的安全体系[5]难以满足物联网轻量级加密要求[6]。与单独和每个组员节点独立加密/认证方式相比, 基于组密钥的安全体系可以避免信息重复发送, 从而提升通信效率。

近年来, 学术界越来越关注物理层安全的研究, 探究在无线网络物理层增强安全性的方法[7]。随着研究的深入, 基于信道特征的密钥生成方法[8], 及基于射频指纹的设备认证[9-11]等安全技术趋于成熟, 物联网多用户的物理层密钥生成方法受到学术界和工业界关注[12-13]。

然而, 若考虑组播的多用户通信需求, 由于不同用户间信道的差异, 利用信道指纹生成密钥则要求设计更复杂的通信协议, 以传递探测信息及共识协商结果, 从而在多用户达成统一密钥源之后才能生成密钥。另一方面, 射频指纹作为设备的固有特性, 在设备认证领域的研究越来越深入, 将射频指纹作为组密钥生成的密钥源的可行性还有待进一步探究。

1.2 相关研究工作

目前, 物理层组密钥的生成方案主要是基于两用户密钥生成的结果, 利用网络拓扑将用于生成组密钥的随机源信息传递到每一个用户节点, 用户节点利用共同特征生成密钥。这里的共同特征可以是本地生成的秘密信息[14], 也可基于两用户密钥生成的信道指纹测量信息[15]。在没有密钥管理中心的条件下, 类似分布式记账, 可通过星形拓扑网络[16]、环式拓扑网络[14]或网状拓扑网络[17-18]来传递随机密钥源, 在组播用户间建立一致的密钥源信息。

文献[8]指出无线信道具有互易性、时变性、空间去相关性的特点, 通信双方在相干时间内可以利用信道信息提取密钥, 而针对半波长以外的窃听方, 测得的信道信息是与合法信道不相关的。在物理层安全的研究中, 利用信道指纹提取密钥常用于两用户通信场景。最近关于射频指纹的研究中已考虑基站利用智能超表面(Reconfigurable Intelligent Surface, RIS)构建快速随机变化的信道的情形, 例如, 文献[19]中研究了基于 RIS 射频指纹密钥产生方法, 其理论与仿真结果表明利用无线信道特征的密钥生成可实现“一次一密”的最优速率。

为了解决多节点场景下信道不同的问题, 目前的研究主要思路是在组播用户间传递两两用户的信道信息, 用户得到共同的先验信息后利用该信息生成密钥。文献[20]考虑三个节点的通信场景, 所有设备发送探测信号给其他设备, 得到了每个设备间的信道冲激响应, 利用该信息量化数据, 生成密钥。仿真结果表明, 该方案窃听成功概率为零。但是, 这种方案仅适用于三用户场景, 在四用户以上场景中, 用户不能获得其他通信用户的信息, 导致方案失效。针对更多用户场景, 文献[17]提出利用中继在多用户间传递信道差异, 进而组播用户基于所得信息生成密钥。文献[17]中还分析了环式网络与星型网络传递信道指纹信息时的密钥生成性能。

综上所述, 如何改进传递信息的方式与中继传递信息的网络模型是影响密钥生成速率、密钥不一致率等安全性能的关键。然而, 基于中继或相互探测的方案有两点不足。一是在传递信道信息时, 需要在节点间多次进行传输, 这个过程中容易收到窃听或攻击。另外, 由于用户间的信息传递, 导致生成密钥的时间增长, 密钥生成速率大大降低, 达不到“一次一密”的性能极限。利用信道指纹生成组密钥需要每个节点获得相同的信道指纹信息作为密钥随机源。但是, 在所有节点取得相同的随机源的过程中, 多个节点需要完成可信的协商通信过程。这个过程不仅消耗能量, 还存在泄露风险。所以, 基于信道指纹的组密钥生成方案有其天然的设计缺陷。文献[21]中指出物联网场景下, 利用射频指纹的安全认证方案相较于传统的基于密码学的认证方案有较低的有效能量密度。考虑到物理层组密钥生成方法, 利用射频指纹生成组密钥则可以提升组密钥生成流程的安全性。

早在 1977 年, 美军海军实验室就开始研究特定辐射识别(Specific Emitter Identification, SEI)技术[22], 即射频指纹的前身。2003 年, 加拿大学者 Hall 等首次提出无线设备的射频指纹(Radio Frequency Fingerprinting, RFF)的概念, 并将其定义为一种基于发射机发射信号瞬态部分对发射机进行识别的技术[11]。目前, 学术界[23-30]认为射频指纹是射频发射机的硬件固有特征对发射的信号产生的独特影响。这些特征来自于设计制造过程中产生的缺陷, 包括数模转换器、带通滤波器、混频器和功率放大器等器件的

微小差异都会使信号产生畸变。这就导致了即使同规格的设备产生相同的信号也是有差异的。

2008 年, 在 Kennedy 等人[23]提出了利用稳态信号进行指纹识别的方法之后, 文献[24-30]提出了利用人工智能技术提升射频指纹识别精度的系列方法。文献[24-26]采用将采集到的时域数据分割成小段, 将 IQ 两路数据作为样本输入深度神经网络, 取得了良好的结果。文献[27]将采集到的时域数据转化为三维表示, 将三维表示的某一段输入网络, 识别精度在某些情形下可达 99%。基于时域数据的人工智能方案虽然识别潜力较高, 但对模型敏感度大, 需要选取合适的网络模型才有较好的识别效果。文献[28]考虑数模转换器、变频器等器件的射频误差, 将信号建模后, 提取特征结合神经网络进行识别, 识别精度接近 99%。类似的, 文献[29]着重考虑 IQ 不均衡与相位噪声, 建立损伤模型, 并进行了仿真与实验, 识别准确率也可达到 99%。文献[30]将时域数据进行变换后, 利用时间序列差分关系的二维表征作为特征进行识别, 对 54 个设备的识别准确度可达 99.1%。

基于上述研究成果, 针对医疗器械组网问题, 文献[31]提出将射频指纹加入组密钥生成过程, 以保障信息传递安全性。虽然, 该方案提高了互联网场景中组密钥生成过程安全性, 但仍未解决多用户信道探测时间消耗大的问题。

1.3 本文主要贡献与创新

本文针对上述多源组播通信场景中密钥生成的问题, 提出了一种联合利用异或自反性与射频指纹的多源终端信息安全传递方法。其中, 利用异或自反性传递秘密消息的想法来源于利用“棋盘网格”传递隐藏信息的游戏[32]。本文的方法考虑将游戏中的网格作为承载信息的时频资源, 结合射频指纹不易伪装的特点, 利用时频资源信息作为密钥随机源生成组密钥。本文的主要贡献与创新点如下:

(1)针对多源用户传输资源选择与认证问题, 本文提出基于扩频与 RSA 算法结合的方法。RSA 算法的引入不仅能够为组播用户选择传输资源提供依据, 还可以为中心节点利用射频指纹认证其他节点提供对照, 增强安全性能; 相比于传统的基于信道指纹的组密钥生成, 本文所提方法利用射频指纹作为密钥生成随机源, 能大大减少密钥生成时间, 分析发现所提方法更适用于多用户场景;

(2)针对射频指纹识别问题, 本文提出一种基于时频分析与卷积神经网络的识别方法, 经过软件无线电设备验证, 证明了所提方法的有效性;

(3)分析了本文所提组密钥的方法的安全性能, 从密钥生成速率、密钥生成效率等角度分析了所提方法的安全性能, 并在窃听场景下分析了所提方法生成密钥被攻破概率。

2 时频资源格异或自反性密钥生成机理

前文提及, 在多源场景中实现密钥生成的一大难点是在每个节点处形成统一的密钥源。本节简述了基于时频资源格划分并利用异或自反性传递秘密信息的机理, 其本质是实现在多终端中快速达到生成密钥的统一认知。

如文献[32]中所述, 假设一个正方形网格中有 2^{σ} 个格点, 且 σ 满足 $\sqrt{2^{\sigma}} \in Z^{+}$, 将所有格点编号为 $0 \sim 2^{\sigma}-1$, 此时, 每个格点都可以用一个 σ 位的二进制数表示。如图 1 所示, 可以将时频资源的分割映射为网格, 阴影网格代表有终端在该格点发射信号。基于这一机理, 结合异或自反特性, 本文提出了一种组播分布式密钥产生方法, 相比于传统密钥产生方式不需要进行密钥协商, 保密增强等步骤。

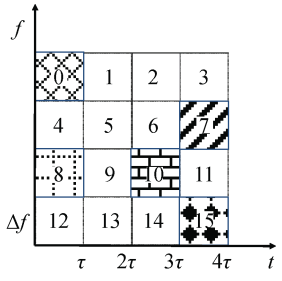


图 1 利用时频资源格传递信息示意图

Figure 1 Conveying information by time-frequency resource grid

以图 1 所示举例, 记 a 为所有在指定时频资源上发送了消息的格点的表示的二进制异或, $a=0\oplus 7\oplus 8\oplus 10\oplus 15$, 此时假设某个格点又发送了一个消息, 记录这个新格点的二进制表示为 b, 假设 b 中包含了秘密消息 s, 即 $b=a\oplus s$, 那么通信组内的其他用户在已知 a 的前提下就可以得到秘密信息 $s=a\oplus b=a\oplus(a\oplus s)$。

3 组密钥生成方法设计

针对如图 2 所示的多源场景下的组密钥生成, 一个中心节点(Central Unit, CU)准备向 k 个边缘节点(Marginal Unit, MU)发起通信, 此时需要一个组内密钥, 保障组内用户准确接收消息, 而组外终端不能接收到消息。根据前文论述, 利用时频资源格与异或的自反性能实现消息的传递。

然而, 若仅依赖时频资源格异或自反性的密钥生成, 从安全脆弱性角度分析, 前文所述秘密分享方法仍存在三个方面的问题: 首先, 在发送消息时没有对每个终端进行身份认证, 容易遭到伪造攻击; 其次, 由于用户时频资源格选择的随机性, 可能会发生信号冲突, 使得多个用户在一个时频资源上发送消息。第三, 针对基于窃听的中间人攻击, 简单的时频资源格异或自反并不能保证安全密钥共享。针对以上问题, 本文提出结合公私钥密钥体系的扩频资源选择方法, 其过程可如图 2 所示。

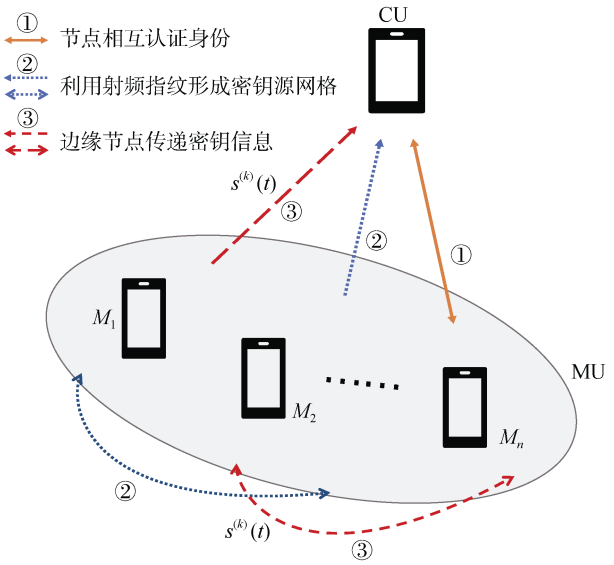


图 2　组密钥生成示意图

Figure 2　Diagram of group key generation

3.1　基于扩频的资源选择方法设计

直接序列扩频技术就是采用高速码率的直接序列伪随机码在发端进行扩频, 在收端采用相同的伪码进行相关解扩。直接序列扩频技术的一大特点是可以实现多个用户的同频工作。由于采用相关解扩, 所以只要每个用户的解扩码不同, 几个用户就可以使用同一载频而不会有互相干扰, 区别在于背景噪声的能量不同。因此, 可以结合公私钥密码体系构建更可靠的资源选择方法。

本节所述的通信资源包括时域、频域与码域(扩频码), 假设一个通信组内的可用时频资源格为 N_R 个, 可选的扩频码序列有 N_G 个, 其中, $(N_R,N_G)=1$, 即可用时频资源格个数与可选的扩频码序列个数互质。设计的需求是组内用户在选择时频资源格与扩频序列时不会发生冲突, 而这一信息在组内是共识。如图 1 所示, 不同的扩频序列用不同的填充表示, 可以看到即便选择了同一时频资源, 扩频码选择不一样仍能区分出不同设备的消息。

由于公私钥密码体系可以满足上述要求, 利用明文生成每个用户的资源索引可以使组内用户已知, 而对于组外用户, 由于其不知道加密信息的内容, 而不能得到每个用户的资源选择。本节选择的加密信息为每个用户的用户编号, 加密方法选择的是 RSA 算法。基于公私钥密码体系的 RSA 算法是一种相对安全的传统加密算法, 但是通过数学算法加密解密, 效率比较低, 比较适合加密比较小的数据, 比较符合多源用户组密钥生成的应用场景。

首先, 在组播通信的选择资源场景中, 每个组成员在首次注册时, 会被分配一个唯一的设备编号。在需要分配资源时, 中心节点首先将私钥 (n,d) 保存在中心节点, 发送公钥 (n,e) 给边缘节点, 边缘节点此时计算明文 $c^{(k)}$,

$$c^{(k)}=M_{id}^{(k)e} \mod n \tag{1}$$

其中, $M_{id}^{(k)}$ 表示第 k 个边缘节点的设备编号。然后根据明文即可计算所用的资源,

$$N_{Rb}^{(k)}=c^{(k)} \mod N_R \tag{2}$$

$$N_{Gc}^{(k)}=c^{(k)} \mod N_G \tag{3}$$

其中, $N_{Rb}^{(k)}$、$N_{Gc}^{(k)}$ 分别表示第 k 个边缘节点选择的时频资源格与扩频码编号。

此时, 每个边缘节点选择了自己所用的时频资源格与扩频码序列。需要注意的是这里的方法不会完全避免资源选择碰撞, 本文将在后面详细讨论。但是由于 $(N_R,N_G)=1$, N_R 与 N_G 互质, 发生碰撞的概率会大大降低。为了使组内其他用户根据时频资源格与扩频码编号得到明文信息, 本文引入节点辅助信息 $m^{(k)}$,

$$m^{(k)}=floor\left(\frac{c^{(k)}}{N_G}\right)-floor\left(\frac{c^{(k)}}{N_R}\right) \tag{4}$$

其中, $floor(\cdot)$ 表示向下取整。

对于在编号为 $N_{Rb}^{(k)}$ 的资源格上, 对于扩频码编号为 $N_{Gc}^{(k)}$ 的用户,

$$\begin{cases} c^{(k)}=floor\left(\dfrac{c^{(k)}}{N_G}\right)\cdot N_G+N_{Gc}^{(k)} \\ \quad\quad =floor\left(\dfrac{c^{(k)}}{N_R}\right)\cdot N_R+N_{Rb}^{(k)} \\ m^{(k)}=floor\left(\dfrac{c^{(k)}}{N_G}\right)-floor\left(\dfrac{c^{(k)}}{N_R}\right) \end{cases} \tag{5}$$

求解可得明文 $c^{(k)}$,

$$c^{(k)}=\frac{N_{Rb}^{(k)}-m^{(k)}N_G-N_{Gc}^{(k)}}{N_G-N_R}\cdot N_R+N_{Rb}^{(k)} \tag{6}$$

根据明文 $c^{(k)}$ 与私钥 (n,d) 可计算设备编号:

$$M_{id}^{(k)}=c^{(k)d} \mod n \tag{7}$$

至此, 完成了边缘节点设备的资源选择, 并在组内所有节点中形成了统一认知。

3.2 组密钥生成方法

本节详述多源场景用户组密钥生成设计方法。本文的方法设计主要包含边缘节点资源选择、节点认证、秘密消息传递方法与组密钥生成四个主要步骤。

具体的密钥生成如图 3 所示, 当中心节点发送组密钥请求后, 会将公钥发送给边缘节点, 此时边缘节点为了验证中心节点的合法性, 同时中心节点会发送射频指纹认证消息。边缘节点首先会依据步骤一的流程完成对中心节点的认证, 并完成资源选择; 接着每个边缘节点在选择的资源上发送射频指纹认证消息与辅助信息, 为了形成对组内其他用户的认证, 此时边缘节点需要监听其他资源上的消息; 之后中心节点根据步骤二所述步骤完成对边缘节点的认证、并根据监听结果生成时频资源使用状态信息网格; 然后中心节点向边缘节点发送组密钥生成确认消息, 表明所有用户认证通过, 可以进行组密钥生成步骤; 为了生成密钥, 每个边缘节点首先根据监听结果同样生成时频资源使用状态信息网格, 并选择自己的秘密格点信息, 并根据步骤三计算自己将要发送的信息隐藏消息, 同时监听其他资源格的消息; 最后所有节点根据步骤四计算秘密格点信息, 并生成组密钥。

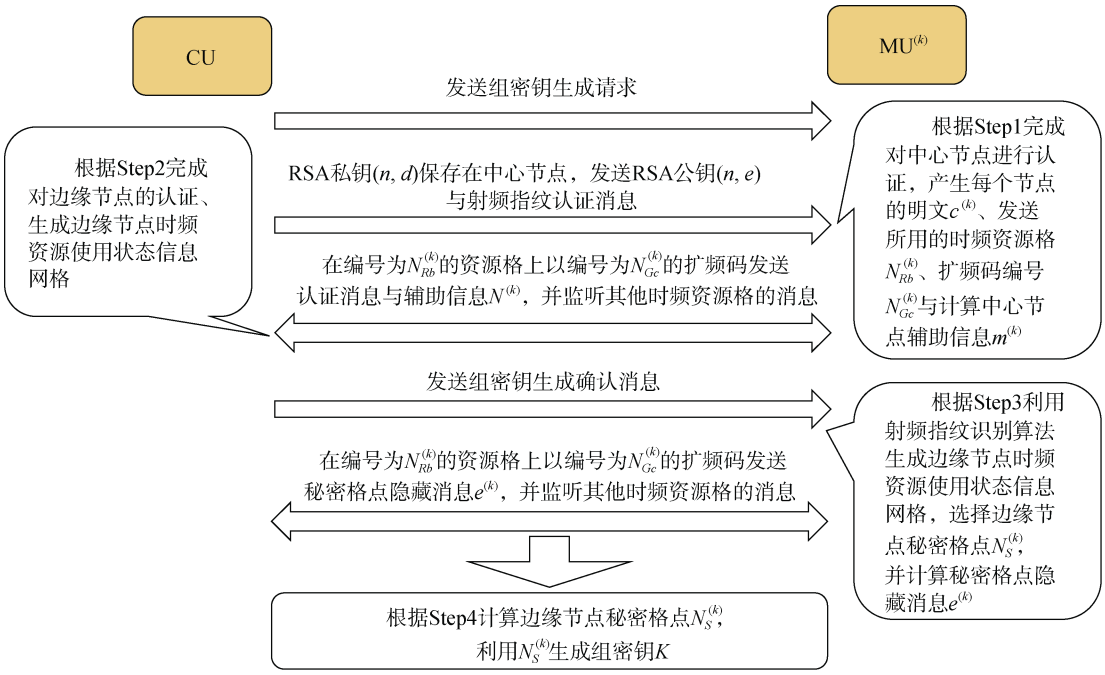


图 3 多用户组密钥生成流程图

Figure 3 Multi-user group key generation process

步骤一: 边缘节点资源选择

(1)边缘节点利用射频指纹识别算法对中心节点进行认证,

$$\hat{M}_{id}^{c}=\mathbb{F}\left(s^{c}(t)\right) \tag{8}$$

其中, $\hat{M}_{id}^{c}$ 表示对中心节点的识别认证结果; $\mathbb{F}(\cdot)$ 表示射频指纹识别算法; $s^{c}(t)$ 表示中心节点发送的射频指纹认证消息。

(2)每个边缘节点根据中心节点发送的公钥计算自己的明文信息 $c^{(k)}$,

$$c^{(k)}=M_{id}^{(k)e} \mod n \tag{9}$$

其中, $M_{id}^{(k)}$ 表示第 k 个边缘节点的设备编号; (n,e) 为中心节点发送的 RSA 公钥。

(3)每个边缘节点根据明文信息 $c^{(k)}$ 计算发送信息所用的时频资源格编号 $N_{Rb}^{(k)}$ 与扩频码编号 $N_{Gc}^{(k)}$,

$$N_{Rb}^{(k)}=c^{(k)} \mod N_R \tag{10}$$

$$N_{Gc}^{(k)}=c^{(k)} \mod N_G \tag{11}$$

其中, N_R 表示总的时频资源格数量, N_G 表示总的扩频码数量。

(4)每个边缘节点根据公式(4)计算节点辅助信息 m^{k} 。

步骤二: 边缘节点认证

(1)在编号为 $N_{Rb}^{(k)}$ 的资源格上, 对于扩频码编号为 $N_{Gc}^{(k)}$ 的用户, 中心节点根据公式(5)～(7)利用私钥 (n,d) 计算每个边缘节点的设备编号 $M_{id}^{(k)}$。

(2)中心节点利用射频指纹识别算法对设备进行识别,

$$\hat{M}_{id}^{(k)} = \mathbb{F}\left(s^{(k)}(t)\right) \tag{12}$$

其中, $s^{(k)}(t)$ 表示第 k 个边缘节点发送的射频指纹认证消息。

(3)中心节点判断是否满足 $\hat{M}_{id}^{(k)} = M_{id}^{(k)}$, 满足说明所有边缘节点认证成功, 否则中心节点认为有非法边缘节点, 重新发送密钥生成请求。

步骤三: 秘密消息传递方法

(1)边缘节点根据监听结果, 在编号为 $N_{Rb}^{(k)}$ 的资源格上, 对于扩频码编号为 $N_{Gc}^{(k)}$ 的用户, 根据公式(12), 利用射频指纹识别算法对设备进行识别。

(2)所有边缘节点根据识别结果生成如图 4 所示的时频资源使用状态信息网格。

(3)每个边缘节点选择一个时频资源网格上的格点作为秘密格点, 记其选择的格点编号为 $N_s^{(k)}$。其中, $N_s^{(k)}$ 为处于 $[0,2^{\sigma}-1]$ 内的二进制表示, $2^{\sigma}=N_R$ 为总的时频资源格数量。

(4)根据时频资源使用状态信息网格, 每个边缘节点计算:

$$A^{(k)} = A \oplus N_{Rb}^{(k)} \tag{13}$$

其中, $A = N_{Rb}^{1} \oplus N_{Rb}^{2} \oplus \ldots \oplus N_{Rb}^{(n)}$ 表示时频资源使用状态信息网格中被边缘节点占用的所有资源格编号的异或。

(5)每个边缘节点计算秘密格点隐藏消息 $e^{(k)}$,

$$e^{(k)} = A^{(k)} \oplus N_s^{(k)} \tag{14}$$

步骤四: 组密钥生成

(1)每个节点监听得到秘密格点隐藏消息 $e^{(k)}$ 后, 利用异或的自反性计算 $N_s^{(k)}$,

$$N_s^{(k)} = e^{(k)} \oplus A^{(k)} = \left(A^{(k)} \oplus N_s^{(k)}\right) \oplus A^{(k)} \tag{15}$$

(2)所有节点计算密钥 K,

$$K = \left(N_s^{(1)}+1\right) \oplus \left(N_s^{(2)}+2\right) \oplus \ldots \oplus \left(N_s^{(n)}+n\right) \tag{16}$$

其中, n 表示总的边缘节点个数。本方法每次生成密钥的长度是由时频资源格的数量决定的, 对于 $N_R = 2^{\sigma}$ 的情况, 每次生成 σ 位密钥。

最后, 由于本方法是基于射频指纹识别的, 为了提高安全性能, 边缘用户在发送认证消息的同时, 还可以在其他时频资源上发送人工噪声, 用来隐藏真实信号, 干扰窃听者对于系统的窃听。

方法有三个关键, 首先是利用基于公私钥密码体系, 完成了在资源(时频域资源与码域资源)上传递了设备编号信息; 其次, 利用射频指纹实现了多源设备的认证, 并将识别结果作为组内用户形成认知的重要前提; 最后, 利用异或的自反性传递秘密消息, 实现密钥生成。

4 射频指纹识别方法

前文提到的组密钥生成方法的基础是射频指纹识别。本节探究射频指纹的识别方法, 并进行实验验证。假设存在 N 个样本, 其设备编号为 $D_1, D_2, ..., D_N$, 其预测编号分别为 $\hat{D}_1, \hat{D}_2, ..., \hat{D}_N$。定义设备识别准确度或精度:

$$R_{Acc} = \frac{\sum_{i=1}^{N}[D_i = \hat{D}_i]}{N} \tag{17}$$

其中, [·] 表示逻辑判断, D_i 与 $\hat{D}_i$ 的值相同时输出为 1, 反之输出为 0。

随着人工智能的发展, 卷积神经网络在图像领域的成功应用使得学者们关注其在射频指纹识别方面的应用[24]。然而射频指纹识别的样本处理方法还有待进一步研究。

4.1 射频指纹识别样本处理方法

4.1.1 基于时域数据的样本处理方法

文献[24]中提出基于时域数据两路数据分离的射频指纹识别样本处理方法。接收机收到的原始信号作为样本便于获得, 且不需要对数据进行额外处理。利用原始 IQ 数据提取设备的射频指纹特征不需要估计信道, 也不需要正在使用的通信协议的任何先验知识。

如图 4 所示, 接收机接收到多个数据包, 在需要识别设备时, 将每个数据包中的数据提取出来, 划

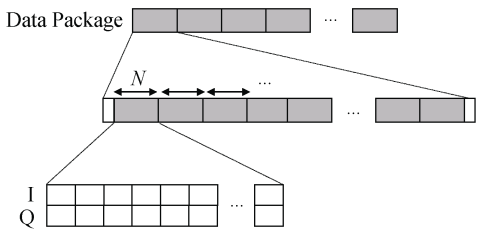


图 4 基于时域原始信号进行射频指纹识别

Figure 4 RFF recognition method based on time domain signal

分成长度相等的信号。将划分好的 IQ 两路信号分离开, 视作信号的两维, 将一个数据包变成了多个样本。类比传统的图像识别, 这里的样本与图像的不同之处在于本文的信号是二维的, 每一维是一路信号, 代表一段时间内接收机接收到的信息; 而图像样本是二维灰度图或三维彩色图像。

4.1.2 基于时频分析的样本处理方法

除了利用时域原始数据进行识别, 射频信号在频域上也具有发射机独特的特征。受到射频指纹瞬态特征研究的启发, 射频指纹通常蕴含在时变的信号中, 信号的功率谱、幅度谱等也是时变的。仅仅了解信号在频域或时域的特征不能完全体现出设备的指纹特征。时频分析能表示出信号频谱随时间变化的信息。短时傅里叶变换(Short-time Fourier Transform, STFT)是最常用的时频分析方法。离散信号的傅里叶变换可以表示为:

$$S[m,k]=\mathcal{F}_s^{\gamma}(m,\mathrm{e}^{j\omega_k})=\sum_n \tilde{s}[n]\gamma^*[n-mN]W_M^{kn} \quad (18)$$

其中, $W_M=\mathrm{e}^{-j2\pi/M}$; $\omega_k=2\pi k/M$, $k=0,1,2,...,M-1$, M 表示频率的离散度; $S[m,k]$ 是定义在样本时间与频率上的二维离散函数。常见的短时傅里叶变换窗函数包括汉明窗、高斯窗与矩形窗, 本文中所用窗函数为矩形窗。

相较于利用时域原始信号进行识别, 基于时频分析的方法更适合利用卷积神经网络进行识别。在实际的识别过程中, 可以将这样一个数据包划分为一个个小样本送入识别网络辨别不同设备的射频指纹。同样的, 短时傅里叶变换的结果同样是复数, 在时频图中显示的是变换结果模的平方, 即:

$$\mathcal{X}[m,k]=|S[m,k]|^2 \quad (19)$$

然而公式(19)的处理会导致该时频点的相位信息消失。所以, 本文采用类似于图像分层的思路, 将时频点上短时傅里叶变换的值实部虚部分开, 看作图像的两层, 将这样的两层数据作为样本利用识别算法对设备进行辨别。

4.2 基于神经网络的射频指纹识别模型

卷积神经网络在发掘样本深层次信息中已经被证明具有较好的应用[33]。本文利用卷积神经网络识别具有不同射频指纹的设备。网络架构与参数设置分别如图 5 和表 1 所示。

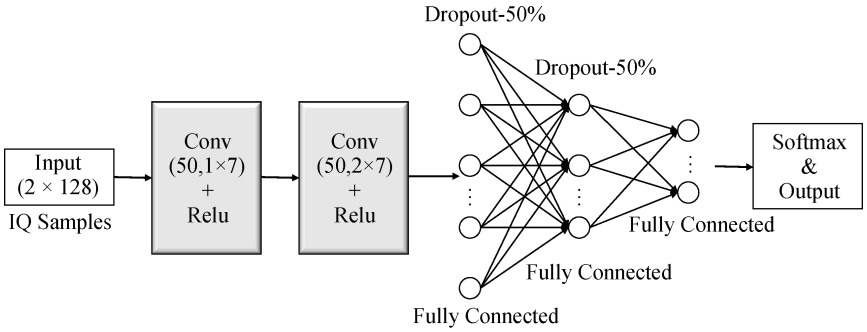


图 5 射频指纹识别卷积神经网络结构图

Figure 5 Structure of convolutional neural network for RFF recognition

表 1 射频指纹识别卷积神经网络参数设置

Table 1 Parameter setting of convolutional neural network for RFF recognition

参数	参数值
第一卷积层	步长为 1, 大小为 1×7, 数量为 50
第二卷积层	步长为 1, 大小为 1×7, 数量为 50
激活函数	ReLU
神经元随机丢弃	50%
批大小	根据样本数量多少决定
学习率	0.0001
损失函数	L2
最大训练轮数	50
损失函数优化算法	Adam

网络的核心为两个卷积层, 包含 50 个卷积核, 其大小分别为 1×7 与 2×7。每个卷积层之后是一个 ReLU 激活函数, 对卷积结果做非线性变换。之后是两个全连接层对卷积层提取的特征做更深度的非线性组合, 其中将 50%的神经元随机丢弃防止过拟合。最后一层使用软分类器输出每个样本被分配给某个标签的概率。

4.3 射频指纹识别仿真与实验平台

目前, 基于软件无线电(Software Defined Radio, SDR)的无线通信技术研究与验证已得到迅速发展, 本节利用通用软件无线电外围设备平台(Universal Software Radio Peripheral, USRP)作为信号收发设备, 模拟物联网多源场景, 对射频指纹识别及基于 USRP

B210[34]的辨识进行了验证。

为完成射频识别技术验证, 需要得到不同的设备的发射数据。本文利用 MATLAB/Simulink 通信工具箱首先模拟了 6 个设备的射频损伤, 这里的射频损伤设置方法主要是人为添加 IQ 不均衡和直流偏移。实验链路采用 QPSK 调制方式, 首先在加性高斯白噪声(Additive White Gaussian Noise, AWGN)信道条件下, 在发送链路中人为加入射频损伤, 测试识别准确率; 之后去除人工损伤, 将基带信号利用 USRP B210 发送出去, 用另一个 USRP 接收, 采集信号后识别不同的设备。

4.3.1 仿真设备链路测试实验

仿真设备链路测试实验链路如图 6 所示, 首先生成数据, 经过调制后人为加入 IQ 不均衡和直流分量, 接收机部分经过滚降滤波器后进行粗频偏校正、符号同步、相偏频偏补偿、帧同步和 QPSK 解调后可以接收到数据。

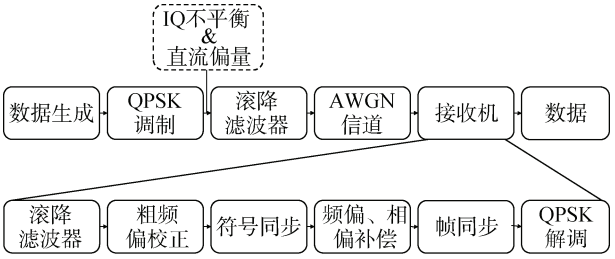


图 6 仿真链路图

Figure 6 Simulation chain diagram

由于 IQ 不均衡与直流偏量是两种最常见的射频损伤, 这里主要设置这两个损伤。

首先按图 7 所示的方法设置了 6 组射频损伤, 记为 C1-C6。其中, β_I 与 β_Q 表示 IQ 两路的不平衡系数; I_{offset} 与 Q_{offset} 分别表示 IQ 两路的直流分量。

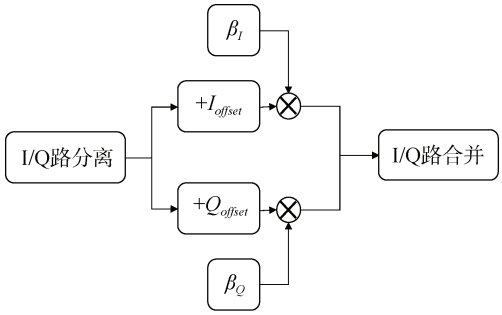


图 7 仿真设备人为损伤设置

Figure 7 Simulation equipment artificial damage setting

具体的射频损伤设置如表 2 所示, 此时不同的仿真设备具有不同的射频损伤, 即带有不同的射频指纹信息。

表 2 射频损伤识别实验仿真设备损伤参数设置表

Table 2 Simulation equipment damage setting table

设备编号	直流偏量		IQ 不平衡幅度	
	I_{offset}	Q_{offset}	β_I	β_Q
C1	0	0	1	1
C2	0	0	1	1.2
C3	+0.2	+0.2	1	1
C4	+0.2	+0.2	1	1.2
C5	0	0	1.2	1
C6	+0.2	+0.2	1.2	1

在如表 3 所示的链路参数情况下, 误码率在10^{-5}量级, 满足通信接收方接收信息的要求, 接收方成功解调出发射机发送的信息。接收机记录经过滚降滤波器后的数据作为识别样本。将接收到的数据按 7∶3 的比例划分训练集与测试集, 采用基于时域原始信号的方法对数据进行识别, 样本长度为 128, 经过训练, 测试集中不同仿真设备的识别准确率为 99.3%。

表 3 射频损伤识别实验仿真设备链路参数表

Table 3 Table of link parameters of rf damage identification experiment simulation equipment

参数	值
帧长度	11226 bits
信息长度	11200 bits
同步头	5
滚降系数	0.5
调制方式	QPSK
信噪比	20 dB

4.3.2 仿真设备链路测试实验测试平台

前文中搭建了射频指纹识别测试链路, 在前文的基础上, 本文设计了射频指纹识别软件无线电测试平台, 整个系统如图 8 所示。

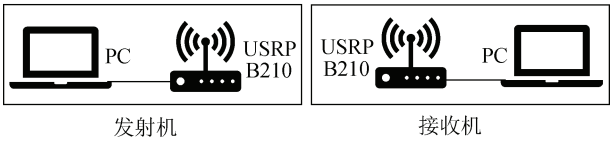


图 8 射频指纹识别软件无线电测试系统示意图

Figure 8 Diagram of RFF recognition SDR platform

利用 Simulink 分别控制两个 USRP B210 作为发射机与接收机, 发射链路与接收链路分别如图 9 与 10 所示。

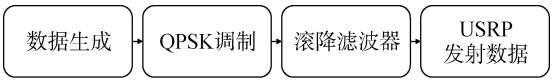


图 9　射频指纹识别软件无线电测试平台发送链路
Figure 9　RFF recognition SDR platform transmit chain

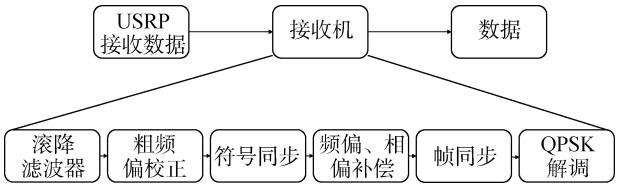


图 10　射频指纹识别软件无线电测试平台接收链路
Figure 10　RFF recognition SDR platform receive chain

相比于仿真数据, USRP 发出的信号的射频损伤来自于不同 USRP 的生产容差, 为了避免接收机射频损伤的影响, 固定用同一个 USRP B210 接收信号。除表 3 中所示的链路参数外, USRP B210 的参数设置如表 4 所示。

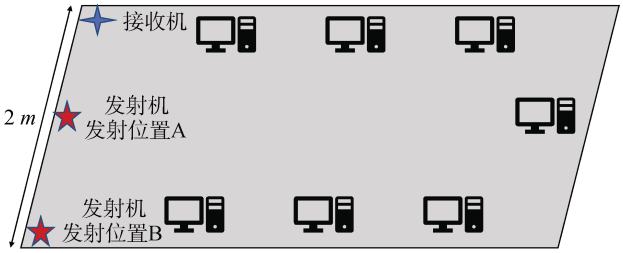
表 4　射频指纹识别软件无线电测试平台 USRP 参数设置表
Table 4　Parameter setting table of RFF recognition SDR platform

参数	值
发射频率	915 MHz
发射增益	25 dB
接收增益	31 dB
基带采样率	40 MHz

本文采用 6 个来自不同的 USRP B210, 将它们作为发射机, 发射相同的信息(“Hello World”), 接收机固定用一个 USRP B210。为了研究在不同信道条件下设备识别的敏感性, 本文还采集了不同距离下的设备信号。

具体的实验场景如图 11 所示。实验时保持信道无遮挡, 保持收发机之间为直视路径, 避免信道情况变化大导致采集到的信号受信道指纹影响过大, 进而削弱射频指纹的特征。接收机位置与接收机设备保持不变, 改变发射机位置。经过测试, 在如图 11 所示的实验场景与表 3、表 4 所示的参数设置下, 作为接收机的 USRP 能正确解调出发射信息。每个发射机分别在如图 11 所示的 A、B 两点处发射信号。

另外, 为了研究接收机对系统影响估计后, 射频指纹识别方法的有效性, 记录了如图 12 所示的不同位置的数据, 即在接收机数据经过滚降滤波器、经过粗频偏校正、经过相偏频偏补偿后的数据。将数据集依次记为数据集一、数据集二与数据集三。此时得到了在 A、B 两点的 6 个数据集。



(a) 测试方法示意图

(b) 测试平台实际场景

图 11　射频指纹识别软件无线电测试平台实验场景
Figure 11　RFF recognition SDR platform experiment scene

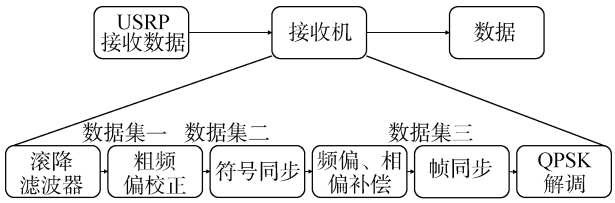


图 12　射频指纹识别软件无线电测试平台数据集采集
Figure 12　Data collection of RFF recognition SDR platform

4.4　射频指纹识别实验识别结果

利用时域原始时域数据与时频分析数据对采集到的信号进行分类, 识别不同的设备, 可以验证算法的有效性。

在这 6 个数据集上[①], 分别将数据集按训练集与测试集按 7∶3 的比例划分, 采用基于原始时域数据的识别方法, 时间长度设置为 128, 每个样本的维度为 2×128。为了研究算法在不同信道条件下的敏感性, 还可将 A、B 两点的数据集合, 在不同信道下对设备进行识别。得到的识别准确率如表 5 所示。

① 数据集及本文代码见 https://github.com/MJTLON/SPZW

表 5 射频指纹识别软件无线电测试平台识别准确率总结表

Table 5 Summary table of recognition accuracy of RFF recognition SDR platform (%)

识别准确率	数据集一	数据集二	数据集三
A 点	94.1	90.6	93.0
B 点	82.5	78.1	93.0
A、B 点混合	81.7	76.8	92.7

另外, 本文还采集了在没有设备发射信号时接收机的接收信号(即噪声信号), 在识别中加入这类信号, 结果显示算法能 100%准确分类出噪声信号, 即算法的虚警概率为 0。

分析表 5 结果发现, 在发射机与接收机距离较近时(发射机位于 A 点), 信号信噪比高, 使用接收机不同位置处采集的数据集识别不同设备均具有较好的识别结果; 当发射机与与接收机距离较远(发射机位于 B 点)时, 信道条件变差, 此时使用接收机将数据进行了相偏频偏补偿后的数据识别设备时准确率较高, 相较于接收机其他位置接收的数据, 识别准确率提高了 10%以上; 最后, 发射机不同位置的数据集联合识别时, 发现识别准确率与距离较远时的结果较为接近, 所以本文提出的射频指纹识别方法的性能取决于信道条件最差时采集数据集的性能。

最后, 本文测试了利用时频分析方法对以上数据集进行识别, 结果显示在每个数据集上, 识别结果均能达到 100%。这进一步证明了本文提出的基于时频分析的射频指纹识别方法更具优越性。

5 安全性分析

本文提出的组密钥生成方法依赖射频指纹识别的性能, 其本质是将设备的射频指纹作为组内用户“认识”其他用户的方法, 然而, 已有研究[21-22]表明, 射频指纹识别仍存在误差。本节将对组密钥生成方法进行性能分析, 研究射频指纹识别准确率对于方法的影响, 并进一步分析了算法关键参数对生成密钥的性能的影响。

5.1 多用户传输资源选择冲突分析

假设边缘用户的数量为 N_{mu}, 有 N_G 个扩频序列, N_R 个时频资源格。边缘用户扩频序列选择有 ${N_G}^{N_{mu}}$ 种选择, 时频资源格有 ${N_R}^{N_{mu}}$ 种选择方法, 即边缘用户共计有 ${N_R}^{N_{mu}} \cdot {N_G}^{N_{mu}}$ 种选择方法。

当所有边缘用户选择的传输资源不冲突时, 对于选择同一个扩频码序列的用户, 时频资源格选择必然需要不同, 从扩频码选择开始入手, 对于 ${N_G}^{N_{mu}}$ 种扩频码选择方法, 对于每一种扩频码选择方法, 必须满足选择每种扩频码的边缘用户数量 k_{i*} 的和为 N_{mu}, 即:

$$N_{mu} = \sum_{i=1}^{N_G} k_{i*} \tag{20}$$

对于第 j 种扩频码选择方法, 假设选择第 $i(i=1,2,\cdots,N_G)$ 个扩频序列的边缘用户数量为 k_{ij}, 那么这 k_{ij} 个边缘用户需要选择不同的时频资源格, 即有组合数 $A_{N_R}^{k_{ij}}$ 种可能情况, 那么对于第 j 种扩频码选择方法, 就有 $\prod_{i=1}^{N_G} A_{N_R}^{k_{ij}}$ 种情况。

所以对于 N_{mu} 个边缘用户, N_G 个扩频序列, N_R 个时频资源格, 所有边缘用户选择的传输资源正交(时频资源格选择或扩频序列选择不冲突)的概率为:

$$p_{\text{orth}} = \frac{\sum_{j=1}^{{N_G}^{N_{mu}}} \prod_{i=1}^{N_G} A_{N_R}^{k_{ij}}}{{N_R}^{N_{mu}} \cdot {N_G}^{N_{mu}}} \tag{21}$$

其中, k_{ij} 表示在共计 $N_G^{N_{mu}}$ 的第 j 种边缘用户选择扩频码情况下, 选择第 i 个扩频序列的边缘用户的个数。

5.2 射频指纹识别对密钥生成效率的影响

根据密钥生成流程, 首先需要进行中心节点认证, 若平均识别准确率为 R_{Acc}, 有中心节点认证成功率:

$$R_{cp} = P\left(N_s = N_{mu}\right) = {R_{Acc}}^{N_{mu}} \tag{22}$$

其中, N_s 表示边缘节点成功认证中心节点的数量。

其次需要选择传输资源, 根据前面推导, 有边缘用户选择的传输资源正交(时频资源格选择或扩频序列选择不冲突)的概率:

$$p_{\text{orth}} = \frac{\sum_{j=1}^{{N_G}^{N_{mu}}} \prod_{i=1}^{N_G} A_{N_R}^{k_{ij}}}{{N_R}^{N_{mu}} \cdot {N_G}^{N_{mu}}} \tag{23}$$

然后中心节点对边缘节点进行认证, 有中心节点认证成功率:

$$R_{mp} = P\left(N_m = N_{mu}\right) = {R_{Acc}}^{N_{mu}} \tag{24}$$

其中, N_m 表示中心节点成功认证边缘节点的数量。

最后中心节点间相互识别, 实现秘密信息传递, 此时每个边缘节点需识别除自身外其余节点, 那么每个边缘节点识别成功其他节点的成功率:

$$R_{op} = P\left(N_a = N_{mu} - 1\right) = {R_{Acc}}^{N_{mu}-1} \tag{25}$$

其中, N_a 表示边缘节点识别成功其他节点的数量。

于是对于所有节点, 全部识别成功的成功率:

$$R_{ap}=R_{op}^{N_{mu}}=R_{Acc}{}^{N_{mu}{}^2-N_{mu}} \tag{26}$$

对于一次密钥生成, 成功生成密钥的概率:

$$\begin{aligned}p_k&=R_{cp}\cdot p_{\text{orth}}\cdot R_{mp}\cdot R_{ap}\\&=\frac{\left(\sum\limits_{j=1}^{N_G{}^{N_{mu}}}\prod\limits_{i=1}^{N_G}A_{N_R}^{k_{ij}}\right)\cdot R_{Acc}{}^{N_{mu}{}^2+N_{mu}}}{N_R{}^{N_{mu}}\cdot N_G{}^{N_{mu}}}\end{aligned} \tag{27}$$

则使用该方法成功生成密钥需要的次数 N_v 的期望 $E(N_v)=\dfrac{1}{p_k}$。

表 6　方法安全性仿真参数表

Table 6　Simulation parameters table of proposed method

参数	值
时频资源格数	64
扩频码数量	16
边缘节点数量	5
RSA 算法明文长度	8 bits
仿真次数	10^5

为了反映射频指纹识别准确率对密钥成功生成概率的影响, 本文做了仿真实验, 实验参数如表 6 所示。其中, 设置时频资源格数量与扩频码数量互质, 能减小资源选择碰撞的概率; 边缘节点数量设置为 5 个, RSA 算法加密的明文长度, 即设备编号设置为 8 比特二进制数。根据目前的射频指纹相关研究, 识别准确率基本能达到 99%以上, 本文考虑射频指纹识别准确率从 99%～100%时方案的性能。

图 13 中展示了射频指纹识别准确率 99%～100%时组密钥生成过程中各步骤成功完成的概率。可以看到, 随着识别准确率的提升, 能显著提高密钥成功生成的概率。由于密钥生成的流程是串联关系, 所以后一流程的成功率会低于前一流程的成功率。最后, 密钥成功生成概率的理论值相较于仿真结果会有 4%的差距, 这是由于边缘节点的资源选择冲突造成的。虽然在方法设计过程中考虑了冲突, 将时频资源格数量与扩频码数量设置为互质, 但仍有选择冲突的概率, 在表 6 所示的参数设置下, 冲突的概率为 4%。

图 14 展示了仿真条件下, 成功生成密钥期望的方法执行次数, 即由于系统设计或射频指纹识别的精度导致需要执行密钥生成方法的次数, 根据结果显示, 在识别准确率为 99%时, 平均需要执行 1.4 次密钥生成步骤才能生成组密钥; 而对于射频指纹能够准确识别的情况, 由于资源选择的冲突, 导致也不能完美生成密钥, 平均需要执行 1.04 次密钥生成步骤才能生成组密钥。

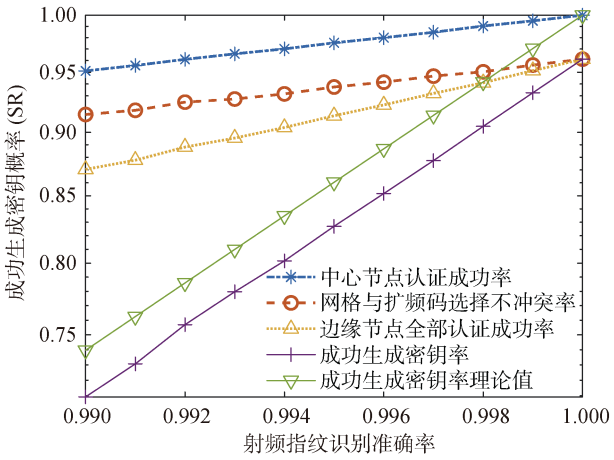


图 13　射频指纹识别与密钥生成效率关系图

Figure 13　The relationship between RFF recognition accuracy and key generation efficiency

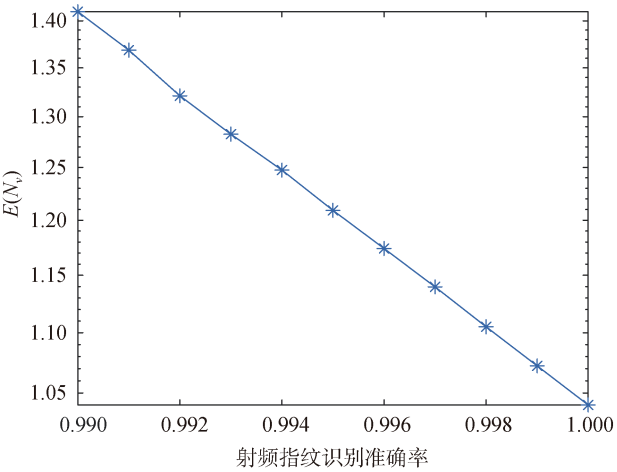


图 14　射频指纹识别与生成密钥方法期望重传次数关系图

Figure 14　The relationship between RFF recognition accuracy and expected number of retransmissions

5.3　组密钥生成速率分析

在物理层安全的研究中, 密钥生成速率(Secret Key Generation Rate, SKGR)是一个重要的衡量指标, 密钥生成速率影响了密钥的更新速率, 从“一次一密”的观点来看, 密钥生成速率的提高意味着可以更快地更新密钥, 以更快的速率发送信息, 提高消息传递效率。

与传统的物理层安全研究不同, 本文设计的组密钥生成方法的密钥生成速率是可调的, 当时频资源格数量 $N_R=2^{\sigma}$ 时, 每次生成长度为 σ 的密钥, 密钥生成速率可以表示为:

$$r_{RFF}=\frac{\sigma}{\alpha\tau}=\frac{1}{\tau} \tag{28}$$

其中, α 表示时间轴上时间资源格的个数, 即 $\sqrt{2^{\sigma}}$; τ 表示一个时频资源格占用的时间。另一方面, 传统的基于中继的组密钥生成方法需要经过信道估计、中继协作和密钥协商来完成[35]。

文献[36]中分析了星型网络与链型网络组密钥生成方法。针对星型网络, 组内节点中心节点与边缘节点轮流发送已知的信道探测信号, 中心节点得到与边缘节点间的信道指纹, 边缘节点得到与中心节点间的信道指纹。之后中心节点选取私密随机源 h_0, 向其他节点协商信道信息, 使组内用户获得密钥随机源。其最大可达速率可以表示为:

$$R_{star}=\lim_{\Delta\to 0}\frac{1}{T}I\left(\tilde{h}_{0,M_c};\tilde{h}_{0,M_1}\right) \tag{29}$$

其中, $\tilde{h}_{0,M_c}$ 与 $\tilde{h}_{0,M_1}$ 表示中心节点与第一个边缘节点对 h_0 的观测值; T 表示相干时间; Δ 表示量化间隔。

假设 τ' 与 τ'' 分别表示完成一次密钥协商或信道探测的最小时间, 则在时分双工(Time Division Duplex, TDD)模式下, 基于星型网络方法的 SKGR 可以表示为:

$$r_{star}=\frac{1}{n\tau'+(n-1)\tau''} \tag{30}$$

针对链型网络, 组内节点轮流向相邻节点发送探测信号, 之后选取一个信道作为私密信道 h_c, 将私密信道的信息共享至其他节点, 使组内用户获得密钥随机源。其最大可达速率可以表示为:

$$R_{chain}=\lim_{\Delta\to 0}\frac{1}{T}I\left(\tilde{h}_{c,M_c};\tilde{h}_{c,M_1}\right) \tag{31}$$

其中, $\tilde{h}_{\mathrm{c},M_c}$ 与 $\tilde{h}_{\mathrm{c},M_1}$ 表示中心节点与第一个边缘节点对 h_c 的观测值; T 表示相干时间; Δ 表示量化间隔。

假设 τ' 与 τ'' 分别表示完成一次密钥协商或信道探测的最小时间, 则在 TDD 模式下, 基于链型网络方法的 SKGR 可以表示为:

$$r_{chain}=\frac{1}{(n-1)(\tau'+\tau'')} \tag{32}$$

对比本文所提方法与传统基于信道指纹的密钥生成方法, 本文所提方法的密钥生成速率大大降低。

5.4 窃听场景安全性分析

传统意义上, 攻破长度为 σ 的密钥需要遍历 2^{σ} 种情况才能完全破解一个未知的密钥。定义密钥被攻破概率 P 如下:

$$P=\frac{1}{N_c} \tag{33}$$

其中, N_c 表示完全破解一个未知密钥需要遍历的数量。

针对合法接收用户, 以一个时频资源格为例, 第 j 个边缘节点接收到的信号可以表示为:

$$s_j(t)=\sum_{k=1}^{n}D(1\|0)h_{jk}s^{(k)}(t)z^{(k)}(t)+n(t) \tag{34}$$

其中, $D(1\|0)$ 表示取 0 或 1; h_{jk} 表示第 j 个边缘节点与第 k 个边缘节点间的信道; $s^{(k)}(t)$ 与 $z^{(k)}(t)$ 分别表示第 k 个边缘节点发出的信号与扩频码序列。进一步的, 用户利用扩频码区分出不同用户, 有:

$$\begin{aligned}&s_{jk_1}(t)=h_{jk_1}s^{(k_1)}(t)+N(t)\\&s_{jk_2}(t)=h_{jk_2}s^{(k_2)}(t)+N(t)\\&\cdots\end{aligned} \tag{35}$$

其中, $N(t)$ 表示等效噪声。

合法接收方可利用射频指纹识别算法对设备进行识别:

$$\hat{M}_{id}=\mathbb{F}\left(s_{jk_x}(t)\right) \tag{36}$$

而对于窃听者, 在一个时频资源上接收到的信号可以表示为:

$$s_e(t)=\sum_{k=1}^{n}D(1\|0)h_{ek}s^{(k)}(t)z^{(k)}(t)+n(t) \tag{37}$$

其中, $D(1\|0)$ 表示取 0 或 1; h_{ek} 表示窃听方与第 k 个边缘节点间的信道; $s^{(k)}(t)$ 与 $z^{(k)}(t)$ 分别表示第 k 个边缘节点发出的信号与扩频码序列。进一步的, 用户利用扩频码区分出不同用户, 有:

$$\begin{aligned}&s_{ek_1}(t)=h_{ek_1}s^{(k_1)}(t)+N(t)\\&s_{ek_2}(t)=h_{ek_2}s^{(k_2)}(t)+N(t)\\&\cdots\end{aligned} \tag{38}$$

由于没有预训练网络 $\mathbb{F}(\bullet)$, 无法通过得到的信号获得设备编号, 所以需要根据接收到信号推测设备射频指纹来获得设备编号。

在表 6 所示的参数下, 每次可生成 6 位的密钥, 若窃听者采用遍历密钥空间的方法破解密钥, 每次生成的密钥被攻破概率为 1.56%。

假设窃听者从密钥生成方法角度出发, 利用射频特性的不同进行破解, 窃听者需要足够的监听获得不同终端的射频特征数据库, 才能完全破解。窃听者先要从随机的资源网格中遍历, 寻找正确的时频资源使用状态信息网格; 其次, 监听者需要监听秘密格点隐藏消息 $e^{(k)}$, 根据遍历得到的时频资源使用状态信息网格 A, 遍历每个节点的 $A^{(k)}$, 进而计算

$N_s^{(k)}$，此后才可破解密钥。

首先，针对 n 个边缘节点，在 g 个时频资源格点上添加了人工噪声来隐藏真实终端信息，则窃听方有组合数 C_{n+g}^{n} 种情况需要遍历；之后，窃听方对 n 个终端资源排列组合，得到每个节点的 $N_s^{(k)}$，所以密钥被攻破概率:

$$P=\frac{1}{A_{n+g}^{n}} \tag{39}$$

若考虑更极端的情形，比如窃听方已统计得到了 N_x 个设备的射频特征，此时窃听方只需要遍历 $C_{n+g}^{n-N_x}$ 种情况。之后，只需要对 $n-N_x$ 个终端排列组合，所以密钥被攻破概率为:

$$P=\frac{1}{A_{n+g}^{n-N_x}} \tag{40}$$

综上可知，影响密钥安全性能的因素包括射频特征遭到泄露节点的个数、添加人工噪声格点的数量和边缘节点总的数量。通过定量分析，以下内容在具体参数下分析了密钥安全性能，研究了射频特征遭到泄露节点的个数、添加人工噪声格点的数量和边缘节点总的数量对组密钥安全性的影响。

在设置人工噪声格点数为 5 的情况下，图 15 展示了射频特征泄露终端数量与密钥被攻破概率的关系，横轴表示射频指纹特征泄露的终端数量，纵轴表示窃听场景下密钥被攻破的概率。观察图 15 发现，窃听者搜索射频指纹特征来破解密钥的成功率复杂度要比遍历密钥所有情况复杂 10 倍以上。随着射频特征遭到泄露节点个数的增加，组密钥的安全性会下降，每增加一个边缘节点的射频特征，密钥被破解概率增加约一个量级；在边缘节点的最后两个节点的射频特征遭到泄露时，密钥被攻破概率将迅速增长，组密钥安全性也随之下降。所以，在组密钥生成过程中，至少要保证两个边缘节点的射频特征没有遭到泄露。

在图 16 中展示了添加人工噪声节点数与密钥被攻破概率的变化关系。首先，随着添加人工噪声格点数的增加，密钥的安全性会显著提升，对于存在 7 个边缘节点(含一个射频特征遭到泄露的节点)的场景，增加一个人工噪声格点能使安全性能增大 2～3 倍；其次，在边缘节点数量比较少的情况下，密钥被攻破概率的下降速度要高于节点数量多的情况，这说明了对于边缘节点数量比较小的场景，加入人工噪声对提高组密钥的安全性的帮助更大。

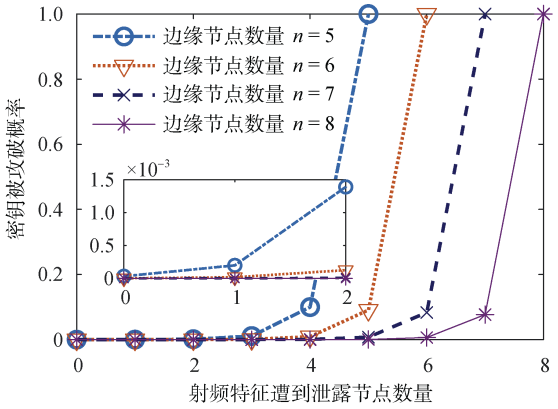


图 15　射频特征泄露终端数量与密钥被攻破概率的关系图

Figure 15　The relationship between the number of RFF leakage terminals and the probability of key cracking

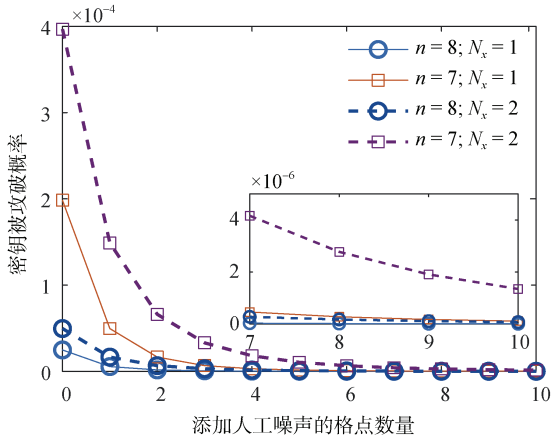


图 16　添加人工噪声节点数量与密钥被攻破概率的关系图

Figure 16　The relationship between the number of artificial noise nodes and the probability of key cracking

在图 17 中展示了在没有边缘节点射频特征泄露时，边缘节点数量与密钥被攻破的概率关系图。从图中可以看到，组密钥的安全性会随着边缘节点数量增加而增加。相比于传统的物理层组密钥生成方法，随着边缘节点数量增加，会使密钥生成更加复杂，中继节点需要传递更多的信息，导致不必要的资源消耗，本文设计的方法不仅规避了这个问题，而且还利用了边缘节点数量多的特点提升组密钥安全性能。

6　结论

针对基于信道指纹的组密钥生成效率低、能耗大且设计复杂的问题，本文提出并论证了一种基于

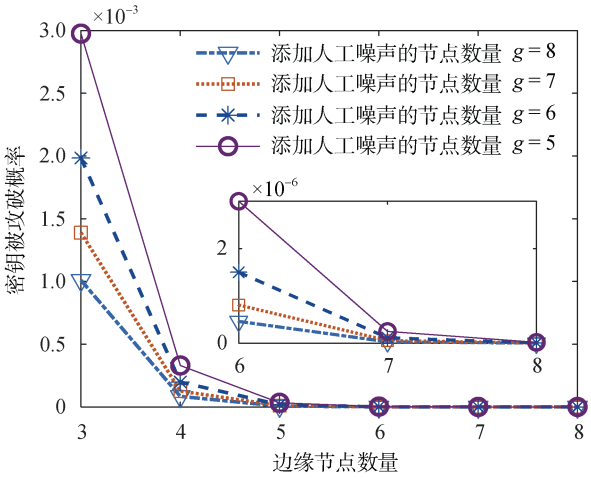


图 17　边缘节点数量与密钥被攻破概率的关系图

Figure 17　The relationship between the number of marginal unit and the probability of key cracking

异或自反性的秘密消息传递方法, 提出利用射频指纹生成组密钥的方法。针对多源用户传输资源选择与认证问题, 本文提出了基于扩频与公私钥密码 RSA 算法结合的方法。区别于传统物理层安全组密钥生成方法, 本文所设计方法能在边缘节点增多的情况下获得更强的安全能力。

射频指纹识别技术是本文提出的组密钥算法的基础, 本文针对射频指纹识别提出了识别算法, 并对算法进行了实验验证, 实验结果证明在本文的实验条件下, 利用本文算法可以识别出不同的硬件设备。

本文相关研究的后续工作包括所提方法的硬件验证, 尤其需要针对具体无线信号与收发信机, 结合已有射频指纹提取方法, 更全面试验评估安全性能与理论分析的差距及受限因素。另外, 为了进一步加强方法的安全性能, 可以在网格上随机加入人工噪声, 干扰非组内用户, 隐藏组内用户射频特征。限于篇幅, 本文并未展开讨论这一问题。

参考文献

[1] Ballardie T. Scalable Multicast Key Distribution[J]. *RFC*, 1996, 1949: 1-18.

[2] Chiou G H, Chen W T. Secure Broadcasting Using the Secure Lock[J]. *IEEE Transactions on Software Engineering*, 1989, 15(8): 929-934.

[3] Wallner D, Harder E, Agee R. Key management for multicast: Issues and architectures[R]. RFC 2627, 1999.

[4] Wu M L, Wang K, Cai X Q, et al. A Comprehensive Survey of Blockchain: From Theory to IoT Applications and beyond[J]. *IEEE Internet of Things Journal*, 2019, 6(5): 8114-8154.

[5] Li H. Security of wireless communication[M]. Beijing: Beijing University of Posts and Telecommunications Press, 2018.
(李晖. 无线通信安全[M]. 北京: 北京邮电大学出版社, 2018.)

[6] Aman M N, Basheer M H, Sikdar B. Data Provenance for IoT with Light Weight Authentication and Privacy Preservation[J]. *IEEE Internet of Things Journal*, 2019, 6(6): 10441-10457.

[7] Shiu Y S, Chang S Y, Wu H C, et al. Physical Layer Security in Wireless Networks: A Tutorial[J]. *IEEE Wireless Communications*, 2011, 18(2): 66-74.

[8] Lei J, Chen W, Li W. A Survey of Key Generation from Wireless Channels[J]. *Radio Communications Technology*, 2021, 47(1): 57-65

[9] Shaw D, Kinsner W. Multifractal Modelling of Radio Transmitter Transients for Classification[C]. *IEEE WESCANEX 97 Communications, Power and Computing. Conference Proceedings*, 2002: 306-312.

[10] Bonne Rasmussen K, Capkun S. Implications of Radio Fingerprinting on the Security of Sensor Networks[C]. *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm*, 2007: 331-340.

[11] Hall J, Barbeau M, Kranakis E. Detection of Transient in Radio Frequency Fingerprinting Using Signal Phase[J]. *Proceedings of the IASTED International Conference on Wireless and Optical Communications*, 2003, 3: 13-18.

[12] Keoh S L, Kumar S S, Tschofenig H. Securing the Internet of Things: A Standardization Perspective[J]. *IEEE Internet of Things Journal*, 2014, 1(3): 265-275.

[13] Park C S. Security Architecture for Secure Multicast CoAP Applications[J]. *IEEE Internet of Things Journal*, 2020, 7(4): 3441-3452.

[14] Xu P, Cumanan K, Ding Z G, et al. Group Secret Key Generation in Wireless Networks: Algorithms and Rate Optimization[J]. *IEEE Transactions on Information Forensics and Security*, 2016, 11(8): 1831-1846.

[15] Liu H B, Yang J, Wang Y, et al. Collaborative Secret Key Extraction Leveraging Received Signal Strength in Mobile Wireless Networks[C]. *2012 Proceedings IEEE INFOCOM*, 2012: 927-935.

[16] Liu H B, Yang J, Wang Y, et al. Group Secret Key Generation via Received Signal Strength: Protocols, Achievable Rates, and Implementation[J]. *IEEE Transactions on Mobile Computing*, 2014, 13(12): 2820-2835.

[17] Truyen Thai C D, Lee J, Quek T Q S. Secret Group Key Generation in Physical Layer for Mesh Topology[C]. *2015 IEEE Global Communications Conference*, 2015: 1-6.

[18] Thai C D T, Lee J, Prakash J, et al. Secret Group-Key Generation at Physical Layer for Multi-Antenna Mesh Topology[J]. *IEEE Transactions on Information Forensics and Security*, 2019, 14(1): 18-33.

[19] Hao Y N, Jin L, Huang K Z, et al. Key Generation Method Based on Reconfigurable Intelligent Surface in Quasi-Static Scene[J]. *Chinese Journal of Network and Information Security*, 2021, 7(2): 77-85.
(郝一诺, 金梁, 黄开枝, 等. 准静态场景下基于智能超表面的密钥生成方法[J]. *网络与信息安全学报*, 2021, 7(2): 77-85.)

[20] Rao M, Harshan J. Low-Latency Exchange of Common Randomness for Group-Key Generation[C]. *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Com-*

munications, 2019: 1-6.

[21] Wu W W, Hu S, Lin D, et al. Reliable Resource Allocation with RF Fingerprinting Authentication in Secure IoT Networks[J]. *Science China Information Sciences*, 2022, 65(7): 170304.

[22] Talbot K I, Duley P R, Hyatt M H. Specific emitter identification and verification[J]. *Technology Review*, 2003, 113: 133.

[23] Kennedy I O, Scanlon P, Mullany F J, et al. Radio Transmitter Fingerprinting: A Steady State Frequency Domain Approach[C]. *2008 IEEE 68th Vehicular Technology Conference*, 2008: 1-5.

[24] Soltani N, Sankhe K, Dy J, et al. More is Better: Data Augmentation for Channel-Resilient RF Fingerprinting[J]. *IEEE Communications Magazine*, 2020, 58(10): 66-72.

[25] Sankhe K, Belgiovine M, Zhou F, et al. ORACLE: Optimized Radio clAssification through Convolutional neuraL nEtworks[C]. *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, 2019: 370-378.

[26] Ding L D, Wang S L, Wang F G, et al. Specific Emitter Identification via Convolutional Neural Networks[J]. *IEEE Communications Letters*, 2018, 22(12): 2591-2594.

[27] Ramasubramanian M, Banerjee C, Roy D, et al. Exploiting Spatio-Temporal Properties of I/Q Signal Data Using 3D Convolution for RF Transmitter Identification[J]. *IEEE Journal of Radio Frequency Identification*, 2021, 5(2): 113-127.

[28] Rajendran S, Sun Z. RF Impairment Model-Based IoT Physical-Layer Identification for Enhanced Domain Generalization[J]. *IEEE Transactions on Information Forensics and Security*, 2022, 17: 1285-1299.

[29] Zhang J Q, Woods R, Sandell M, et al. Radio Frequency Fingerprint Identification for Narrowband Systems, Modelling and Classification[J]. *IEEE Transactions on Information Forensics and Security*, 2021, 16: 3974-3987.

[30] Peng L N, Zhang J Q, Liu M, et al. Deep Learning Based RF Fingerprint Identification Using Differential Constellation Trace Figure[J]. *IEEE Transactions on Vehicular Technology*, 2020, 69(1): 1091-1095.

[31] Mustafa U, Philip N. Group-Based Key Exchange for Medical IoT Device-to-Device Communication (D2D) Combining Secret Sharing and Physical Layer Key Exchange[C]. *2019 IEEE 12th International Conference on Global Security*, *Safety and Sustainability*, 2019: 1-7.

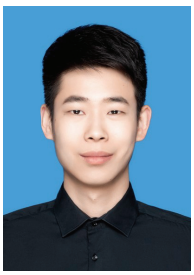
[32] Zilin J. Communicating Information through Randomness[EB/OL]. https://blog.zilin.one/2014/03/06/communicating-information-through-randomness/, March 1, 2022.

[33] Krizhevsky A, Sutskever I, Hinton G E. ImageNet Classification with Deep Convolutional Neural Networks[J]. *Communications of the ACM*, 2017, 60(6): 84-90.

[34] Ettus. USRP B210[EB/OL]. https://www.ettus.com.cn/product/B210kit.htm.

[35] Xiao S F, Guo Y F, Huang K Z, et al. Cooperative Secret Key Generation for Multi-Hop Relaying Systems in Internet of Things[J]. *Journal on Communications*, 2018, 39(3): 86-94.
(肖帅芳, 郭云飞, 黄开枝, 等. 面向物联网多跳中继系统的协作密钥生成方法[J]. *通信学报*, 2018, 39(3): 86-94.)

[36] Xiao S F. Research on Physical Layer Secret Key Generation for Internet of Things[D]. Zhengzhou: Information Engineering University, 2018.
(肖帅芳. 面向物联网的物理层密钥生成技术研究[D]. 郑州: 战略支援部队信息工程大学, 2018.)



开根深 于 2019 年在电子科技大学光电信息科学与工程专业获得学士学位, 于 2022 年在电子科技大学信息与通信工程专业获得硕士学位, 现工作于西安电子工程研究所。研究领域为无线通信与物理层安全。Email: genshen_kai@163.com

马俊韬 于 2021 年在电子科技大学电子信息工程专业获得学士学位。现在电子科技大学信息与通信工程专业攻读硕士学位。研究领域为无线与移动通信系统。Email: 15328790500@163.com

武刚 于 2004 年在电子科技大学通信与信息系统专业获得博士学位。现任电子科技大学通信抗干扰全国重点实验室教授, CCF 会员。研究领域为无线与移动通信、通信抗干扰与网络安全。Email: wugang99@uestc.edu.cn

胡苏 于 2010 年在电子科技大学通信与信息系统专业获得博士学位。现任电子科技大学通信抗干扰全国重点实验室教授。研究领域为 5G/6G 移动通信、抗干扰/低截获无线通信系统、无线通信大数据应用。Email: husu@uestc.edu.cn