# 5G网络空间安全对抗博弈

徐 瑨 吴慧慈 陶小峰*

(北京邮电大学移动互联网安全技术国家工程实验室 北京 100876)

**摘 要**：随着移动通信技术的快速发展和第5代移动通信(5G)网络的商用，网络空间安全问题日益凸显。该文针对5G网络空间安全中对抗博弈问题进行探讨，从静态博弈、动态博弈、基于演化和图论的博弈等基础模型以及窃听与窃听对抗、干扰与干扰对抗等典型对抗种类方面，对当前国内外网络空间安全对抗博弈的研究进行分析和归纳，并进一步阐述5G网络空间安全对抗博弈研究中潜在的基础理论和对抗规律研究方向，分析5G环境下安全对抗博弈研究的必要性及面临的挑战，为5G网络空间安全攻防对抗研究提供新视角。

**关键词**：第5代移动通信；网络空间安全；对抗；博弈

**中图分类号**：TN918; TN929.5 **文献标识码**：A **文章编号**：1009-5896(2020)10-2319-11

**DOI**: 10.11999/JEIT200058

# 5G Cyberspace Security Game

XU Jin WU Huici TAO Xiaofeng

(*National Engineering Laboratory for Mobile Network Technologies*,
*Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)

**Abstract**: With the rapid development of mobile communication technologies and the commercial use of 5G, cybersecurity issues are increasingly prominent. For revealing the essence of operation in 5G cybersecurity, current researches on cybersecurity confrontation and game are analyzed from the aspects of basic models including static game, dynamic game, evolutionary game, and graph-based game, as well as the typical confrontation issues including eavesdropping and anti-eavesdropping and jamming and anti-jamming. Furthermore, some potential research directions are also set forth in establishing 5G cybersecurity confrontation theory and general law. Finally, the necessity and challenges of security and game research in 5G networks are discussed, so as to provide new sights for the research of confrontation in 5G cyberspace.

**Key words**: 5G mobile communication; Cybersecurity; Confrontation; Game

## 1 引言

第5代移动通信(5G)逐渐商用将导致网络空间的进一步扩展，在网络规模、网络层次增加的同时，其安全问题也日趋严峻。一方面，5G 三大应用场景(增强型移动宽带(enhanced Mobile Broad-Band, eMBB)、海量物联网(massive Machine Type Communication, mMTC)和高可靠低时延(ultra Reliable Low Latency Communication, uRLLC))的研发推动5G由移动互联网时代向移动物联网时代转变[1]，网络规模可达每平方千米100万台设备接入，同时，5G网络对各类垂直行业的支持，使得其接入网是一个异构融合的网络[2,3]，不同服务、不同接入方式的安全需求具有很大差异，要求5G安全设计考虑分层次、大规模、多样化的安全管理；另一方面，传统网络设备的安全性很大程度依赖于实际的物理隔绝，而5G网络采用基于软件定义网络(Software Defined Network, SDN)/网络功能虚拟化(Network Function Virtualization, NFV)的新型切片式网络架构[4–7]，在软硬件分离的基础上，实现通用硬件基础设施平台的云化部署，使网络空间边界弱化，软件漏洞、硬件入侵、病毒木马、恶意攻击等问题易于爆发[8–11]，因此要求5G安全设计进一步考虑各虚拟模块之间的安全隔离以及各虚拟网络切片的安全管理。

在万物互联时代，5G异构融合网络的攻击面广，攻击日趋频繁，攻击方式灵活多变，其超高的传输速率和超低的传输时延使得网络攻击能有更快

收稿日期：2020-01-15；改回日期：2020-06-19；网络出版：2020-06-26
*通信作者： 陶小峰 taoxf@bupt.edu.cn
基金项目：国家自然科学基金(61932005, 61901051, 61501057)，中央高校基础科研费专项资金(2019RC55)
Foundation Items: The National Natural Science Foundation of China (61932005, 61901051, 61501057), The Fundamental Research Funds for The Central Universities (2019RC55)

的传播速度，当前的网络空间攻击模型不完全适用于5G时代的网络空间攻击传播机理研究。在网络空间中，计算机病毒、网络谣言等是重要的攻击手段，严重威胁网络空间安全，又严重耗费资源。5G网络覆盖面积广、移动终端普及率高、移动业务多样化、用户身份虚拟，使计算机病毒扩散更快，网络谣言引发更强烈的多链式互动和传播，对现实世界的危害更加明显；5G网络的数据速率是第4代移动通信(4G)的100～1000倍，而端到端的毫秒级时延只有4G网络的1%[12]，快速且大量的信息交互导致计算机病毒和网络谣言的传播一定程度上呈现出爆发性和隐蔽性的特点；此外，多代移动通信网络长期共存，4G/5G的分布式网络将导致攻击传播方式和传播途径更加多样。

网络空间安全的本质是攻击者(黑客)与防御系统(红客)之间的对抗博弈。在5G网络空间安全研究中，一方面，虽然传统的网络安全方法如身份认证、入侵检测、流量监控等仍将在5G系统安全防护方面发挥重要作用，但防御时常滞后于攻击，很难响应5G网络中更为复杂的攻防对抗；另一方面，红客面临更加繁复的攻击，如何统筹兼顾选择恰当的防御策略，在攻击者尚未造成严重损失之前敏捷高效地对网络进行加固并产生攻击响应也是一大难点。5G环境下网络攻击特性的改变将给网络攻击防御研究带来挑战，传统的针对单次攻击事件的研究方法难以有效分析具有爆发性和隐蔽性特征的攻击传播规律。并且，5G网络中的安全对抗将包含人与人、人与机器、机器与机器之间的对抗，兼具非理性对抗与理性对抗。传统的网络安全技术、信息安全方法不完全适用于5G时代的网络空间安全研究，因此，迫切需要研究面向5G网络的网络空间安全对抗基础理论。

近年来，网络安全问题成为信息领域的重要关注点。一方面，针对5G环境下的网络空间安全研究已逐步展开，为安全技术的演进提供了方向性指导，冯登国等人[13]提炼了5G网络安全框架，归纳并阐述了5G网络安全关键问题及其解决方案；Cao等人[14]从5G标准的角度，分析了新特性和新技术为5G网络带来的安全需求和存在的开放性问题；Khan等人[15]分析了基于5G核心技术的安全措施，探讨了5G网络的安全监测和管理，并给出5G及未来网络面临的安全挑战；另一方面，从宏观层面研究网络空间安全理论也受到多国学者的高度重视，Ponniah等人[16]提供了一种可证明安全的无线网络系统论方法；Alpcan和Basar[17]发表著作《Network Security: A Decision and Game-theoretic Approach》，基于博弈论、策略判决和控制论等理论给出了网络安全的系统级理论建模方法；杨义先等人[18]发表了著作《安全通论》，系统阐述了网络攻防对抗中的基础问题。

针对5G环境下的网络空间安全对抗基础理论和对抗规律研究问题，本文第2节对网络空间安全对抗博弈进行了研究现状分析和归纳；在此基础上，第3节基于5G网络架构的特性和安全需求归纳，对网络空间安全对抗博弈研究方向和潜在发展趋势进行分析与讨论，并以5G接入网为例，给出安全对抗博弈研究思路；最后，第4节总结本文。

## 2 网络空间安全对抗博弈研究现状

网络空间安全对抗博弈是黑客和红客彼此不断抗衡和影响的过程，黑客、红客的攻防对抗行为具有：(1)目标对立性：黑客的目标在于实现网络攻击，红客的目标在于防守黑客；(2)策略依存性：黑客的攻击行为与红客的防守行为相互牵制、相互影响；(3)关系非合作性：黑客与红客位于攻防对立面[18]。目前，运用博弈模型分析网络攻防行为，开展防御决策研究已经取得部分成果。

### 2.1 安全对抗博弈基础模型

网络空间安全对抗博弈模型包括静态博弈、动态博弈、演化博弈以及结合图论的博弈等，典型的博弈模型如表1所示。其中，研究静态对抗博弈问题常用的博弈模型有斯塔伯克博弈、贝叶斯博弈、随机博弈、零和博弈等，研究动态对抗博弈问题常用的博弈模型有微分博弈、基于马尔科夫判决的博弈、递阶对策博弈等。实际网络安全攻防场景中的

表 1 典型的网络空间安全对抗博弈模型

| 博弈类型 | 博弈模型 | 参考文献 |
|---|---|---|
| 基于静态博弈的安全对抗 | 斯塔伯克博弈 | [19–25] |
| | 贝叶斯博弈 | [26] |
| | 随机博弈 | [27–30] |
| | 混合策略博弈 | [31] |
| | 零和博弈 | [32,33] |
| | 完全/不完全信息博弈 | [20,26,30] |
| 基于动态博弈的安全对抗 | 完全/不完全信息博弈 | [34,35] |
| | 微分博弈 | [36–38] |
| | 信号传递博弈 | [39] |
| | 基于马尔可夫判决 | [40,41] |
| | 递阶对策 | [42] |
| 基于演化博弈的安全对抗 | 对称/非对称博弈 | [43,44] |
| | 完全/不完全信息演化博弈 | [45] |
| | 马尔可夫演化博弈 | [46] |
| 结合图论的博弈对抗 | 贝叶斯攻击图 | [47] |
| | 概率攻击图 | [48] |

对抗博弈随着攻击与防御实力的改变而不断演化，演化博弈论主要用于研究攻防策略的互动过程；攻击与防御策略的改变和攻防实力的变化通常是在多个状态之间不断转换，结合图论建模网络攻击状态变化，可以更加清晰地刻画攻防对抗及演化过程中策略转移和攻防平衡态的演变。

#### 2.1.1 基于静态博弈模型的安全对抗

基于静态博弈模型，文献[19–25]采用了基于斯塔伯克博弈理论的攻防对抗研究。文献[20]提出了多攻击、单智能防御的数据注入攻击模型，分析了博弈均衡的存在性和性质。文献[21–23]研究了对抗干扰攻击和窃听攻击的博弈问题，提出了基于斯塔克尔伯格博弈欺骗防御策略，在通信系统对于欺骗攻击者全盲和非全盲两种情况下，计算攻击者与防御者之间的斯塔克尔伯格平衡。Li等人[24]研究了防御者和攻击者之间的交互式决策，分析了不同类型预算约束下的决策最优解。Han等人[25]研究了云计算环境下的攻防对抗博弈及其均衡解的存在。La等人[26]运用静态贝叶斯博弈理论构建攻防对抗模型，通过求解静态贝叶斯均衡来实现对最优防御策略的选取。

采用随机博弈模型，Wei等人[28]分析了电网系统中的防御协同攻击的对抗问题，得到了防御者可以采用的最优策略。王元卓[29]等人提出一种基于随机博弈模型的网络攻防实验架构，在此架构下进行各种网络攻防的实验推演，分析网络系统安全性。Doraszelski等人[30]构建多阶段攻防信号博弈模型，研究了有限信息条件下多阶段攻防的防御策略选取问题。

基于混合博弈模型，Xiao等人[31]研究了云存储系统中针对APT的防御问题，分析了混合策略主观存储防御博弈，推导出了攻防博弈的纳什均衡，表明APT攻击者的主观观点可以提高防守者的效用。基于零和博弈，Zhang等人[32]提出了双层博弈模型，提供了网络保险的综合视图，并实现了激励兼容和攻击感知保险的系统设计。Min等人[33]研究了云存储系统中APT攻击者和防御者在多个存储设备上分配CPU的交互。

#### 2.1.2 基于动态博弈模型的安全对抗

Fudenberg等人[49]在《Game Theory》中引入动态博弈模型。网络空间安全攻防对抗是一个多阶段的博弈过程，Laszka等人[34]提出基于多属性效用的博弈模型，假设攻击者了解防御者的所有策略。在完全信息条件下，Wang等人[35]刻画了受控环境下电网系统可能存在的攻防动态特性，提出了攻防之间的边界。基于信号传递模型，Shen等人[39]以在线社交网络为背景，在不完全信息条件下对攻击者行为进行分析。基于微分博弈，Huang等人[36]研究了网络安全状态随机和网络防御策略判决高动态的攻防对抗问题，结合微分博弈模型和马尔可夫决策方法，构造了马尔可夫攻击防御微分博弈模型并进行动态分析，预测多阶段连续攻击防御过程。Zhang等人[37]在借鉴传染病模型的基础上，提出了新的网络安全状态演化模型。在此基础上引入微分对策理论，建立了攻防微分对策模型，通过对博弈均衡的分析，设计了实时对抗中最优防御策略选择算法。Garcia等人[38]研究了零和微分对策在主动目标防御中的应用，提供了一个完整的、封闭的主动目标防御微分对策解。

采用马尔可夫建模攻击者的攻击目标，Maleki等人[40]指出微分博弈是时间实时变化情况下描述冲突对抗中连续控制过程的理论方法，能够刻画系统状态和决策控制的动态连续变化过程，可以更好地分析攻防双方的连续、实时对抗行为，实现最优防御策略动态选取。Lei等人[41]提出了一种移动目标防御(Moving Target Defense, MTD)策略，马尔可夫决策过程用于表征网络多态之间的转换，动态博弈可用于描述MTD情况下攻击和防御的多个阶段。

#### 2.1.3 基于演化和图论博弈模型的安全对抗

演化博弈模型是安全对抗中一类较常用的博弈模型。基于对称和非对称演化博弈理论，Balkenborg等人[43]研究了蠕虫病毒攻击和防御策略的效能。Fiondella等人[44]基于博弈理论漏洞评估技术，分析了遗传算法对防御网络链路的影响，并研究了有限防御资源对网络链路的最优分配。Abass等人[50]通过构建离散策略的演化博弈模型来研究APT攻击行为，进而讨论了攻防策略的动态稳定性。Bharathi等人[51]研究了认知无线网络中对抗响应/无响应干扰攻击的博弈问题。对于最佳网络防御策略选择问题，Hu等人[45]研究了在不完全信息条件下最佳网络防御策略选择，Huang等人[46]研究了基于马尔可夫演化博弈的最佳防御选择。

将攻击者的行为以图论的形式表征，Miehling等人[47]构建了一个基于贝叶斯攻击图的静态博弈模型，通过求解博弈均衡，最终将混合策略均衡作为最优防御策略的选取。采用概率攻击图，陈小军等人[48]对攻防随机博弈中的网络系统安全状态转移模型进行了改进，并在此基础上分别对网络生存性和网络攻击开展研究。

### 2.2 5G无线接入网典型安全对抗博弈

以上经典博弈模型为分析网络空间安全问题与对抗研究提供了基础的研究方法和研究思路。无线接入网作为5G网络的重要组成部分，其安全威胁

和安全对抗是5G网络空间安全研究的一大重要分支，目前5G无线接入网安全对抗博弈相关研究主要集中于物理层安全。

以5G无线接入网中的安全问题与对抗研究为例，表2归纳了无线接入网中典型的窃听与窃听对抗、干扰与干扰对抗两大类攻防对抗研究成果。研究窃听与窃听对抗问题常见的博弈模型包括斯塔伯克博弈、契约理论、拍卖模型、联盟博弈、Bertrand博弈、零和博弈等；研究干扰与干扰对抗问题常见的博弈模型包括斯塔伯克博弈、贝叶斯博弈、协作干扰攻击间的博弈、基于学习的干扰对抗等。

#### 2.2.1 窃听与窃听对抗

窃听攻击是无线接入网中最典型的一类攻击方式，恶意攻击者通过主动或被动的方式非法获取合法链路的无线信号。得益于Wyner 1975年所提3点窃听信道模型，针对于无线接入网的物理层窃听对抗研究备受关注。Han等人[52]最开始采用博弈论思想研究窃听与窃听对抗之间的策略交互，多个友好的、自私的干扰节点通过发送干扰信号恶化窃听信道，Zhang等人[53]采用斯塔伯克博弈模型建立和研究了合法发送节点与干扰节点之间的策略交互，并基于斯塔伯克博弈模型进一步考虑了双向非可信中继场景下友好干扰节点与合法发送节点之间的策略交互。实际通信场景中，合法发送节点一般是配备多天线的基站或者中继节点，Chu等人[54]考虑这一实际问题，研究了多天线系统中合法发送节点与一个干扰节点之间的策略交互。Wu等人[55]则进一步采用单引导者-多跟随者斯塔伯克博弈模型研究了多天线系统中合法发送节点与多个干扰节点之间的策略交互，并分析了信道状态不完全已知情况下的策略交互问题。同样，Fang等人[56]采用单引导者-多跟随者斯塔伯克博弈模型研究了多中继协作场景下的合法发送节点与中继节点之间的策略交互。以上研究中窃听者都是被动窃听，即不采取任何主动措施。Fang和Luo等人[57,59]考虑全双工主动窃听者边窃听保密信号，边发送干扰信号干扰合法链路，在此场景中，Fang等人采用一个多层斯塔伯克博弈模型研究了攻击者和(多个)合法中继之间的对抗交互和竞争交互问题。

为了激励干扰节点的协作，Li等人[60]采用契约理论研究了合法发送节点与干扰节点之间的策略交互问题。斯塔伯克博弈模型一般用于研究一个合法链路和一个或多个协助节点之间的策略交互，在存在多个合法链路和一个协助节点场景中，多个合法链路需要对协助节点进行竞争和拍卖[61,62]。考虑到传统的集中式拍卖模型中玩家存在的自私性和合谋性，Khan等人[63]引入了区块链技术，建立分布式无信任拍卖模型。为了进一步提高抗窃听性能，多用户协作形成合作联盟，以协作波束形式发送保密信号能改善传输保密信号的合法链路质量，Saad等人[64]采用联盟博弈模型研究了协作多用户之间的策略交互。除拍卖模型之外，Wang等人[65,66]进一步采用Bertrand博弈模型研究了合法链路对自私干扰节点或中继节点的选择问题。实际无线通信场景中存在同时具有窃听和对抗窃听能力于一体的节点，文献[67,68]采用零和博弈模型研究和分析了合法链路和窃听链路对此类节点的竞争。

表 2 5G无线接入网中的典型安全对抗博弈

| 对抗种类 | 应用模型 | 参考文献 |
|---|---|---|
| 窃听与窃听对抗 | 斯塔伯克博弈 | [52–59] |
| | 契约理论 | [60] |
| | 拍卖模型 | [61–63] |
| | 联盟博弈 | [64] |
| | Bertrand博弈 | [65,66] |
| | 零和博弈 | [67,68] |
| 干扰与干扰对抗 | 斯塔伯克博弈 | [22,23] |
| | 贝叶斯博弈 | [69] |
| | 协作干扰攻击间的博弈 | [70] |
| | 基于学习的干扰对抗 | [71,72] |

#### 2.2.2 干扰与干扰对抗

干扰攻击在无线接入网络中是一类以发送噪声信号干扰合法链路信道质量的破坏类攻击，其目的在于让合法接收端无法正确解调保密信息。文献[22,23,69–72]研究了无线接入网中的干扰者与对抗干扰者之间的策略博弈，其中Jia等人[23]对对抗干扰研究中的挑战性做了深入分析，包括干扰认知、对抗干扰决策判定以及波形配置等问题，并进一步采用斯塔伯克博弈模型研究了对抗干扰的具体实施步骤，包括功率控制和信道选择问题。Ahmed等人[22]则采用斯塔伯克博弈模型研究了IEEE 802.22认知无线电网络中具有频谱认知能力的干扰攻击者与主用户之间的博弈问题。在一个合法发送节点对其他发送节点信息不完全已知的情况下，Sagduyu等人[69]采用贝叶斯博弈模型研究了概率条件下各合法发送节点之间的接入控制决策交互问题。在存在多个干扰攻击节点场景中，Tang等人[70]引入社交关系来研究各个协作干扰节点之间的策略交互。为了解决对抗干扰问题中纳什均衡的求解，Lü, Lu等人[71,72]引入Q学习和强化学习算法。

### 2.3 小结

本节归纳了网络空间安全研究中的对抗博弈模

型，分别以静态博弈、动态博弈、演化博弈以及结合图论的博弈模型对网络空间中的各类安全威胁和安全对抗研究进行了分析，在此基础上，进一步针对5G无线接入网中窃听与窃听对抗、干扰与干扰对抗两类典型攻防对抗问题，分析并归纳了已有研究成果，展示了国内外相关领域学者在攻防对抗博弈方面的重要研究进展，为网络空间安全攻防对抗提供了有益的研究思路和基础。但从上述分析也可以看出，已有研究较少考虑到5G时代网络攻击的大规模化、攻防一体化、智能化和升级演变等特点，例如，百亿级规模物联网的到来将引发大规模的分布式拒绝服务(Distributed Denial Of Service, DDOS)攻击等，会带来更大的网络宏观效应。因此，针对5G时代网络空间的攻防对抗，需要深入开展宏观角度的攻防对抗研究，以动态博弈、随机博弈、演化博弈等理论模型为基础，研究不断改变的网络环境中的对抗演化过程，实现从整体角度把控攻防对抗演变规律。

## 3　5G网络空间安全对抗博弈研究

### 3.1　5G网络空间安全对抗基础理论研究

针对不同业务场景和应用需求，5G接入网呈现多样化的特点。物联网和车联网的引入，使得服务对象从传统的人与人通信拓展到人与物、物与物通信，且对通信的可靠性、即时性、安全性提出了更高的要求；为支撑异构多样化的接入网需求，进一步提升网络处理能力，增强网络资源的灵活配置，降低网络处理时延，5G网络基于SDN/NFV技术实现了通用硬件基础设施平台，在对传统网络进行软硬件分离的基础上将网络功能虚拟化，并在核心网层面进行统一的云化部署，结合差异化分层思想，实现网络服务的切片式管理和按需组网，如图1所示。5G环境下新增的安全需求包括：SDN/NFV安全、边缘计算安全、物联网/车联网安全等，其网络空间安全对抗相较于传统网络安全对抗更为复杂。为了实现从全局角度把控整个网络空间安全态势，可从5G网络安全对抗模型、对抗演化规律以及安全整体态势感知等方面展开研究。

首先，5G网络空间安全对抗不但要考虑攻防对抗的行为和实力问题，还要结合对抗双方的网络容量等问题，考虑对抗双方的损失演化。一般情况下，大多数网络实体只是具有单一的攻击或防御能力。但在万物互联的5G时代，网络攻防单元通常是攻防一体的：5G网络采用基于SDN/NFV的网络架构，集中式SDN控制器主要完成网络资源的管理和网络业务的动态编排，能实现防护的快速生效。反之，攻击者也可利用SDN实施攻击，造成网络瘫痪；利用NFV可快速部署大量虚拟化安全设备，实现安全策略动态编排，并且可利用虚拟化实现攻防一体。因此，针对5G时代的新型安全对抗模式，需从多个角度和因素分析网络安全单一对抗和一体对抗行为，结合对抗双方之间网络软硬件设施和数据情报，基于博弈论建立5G网络对抗双方之间的对抗架构与博弈模型。

其次，5G网络环境下在线设备接入数量倍增，并且物联网和车联网等加入令网络状况更为复杂，使得各种攻击手段和对抗方法层出不穷，网络状况的发展日新月异，该背景下，可以在构建网络

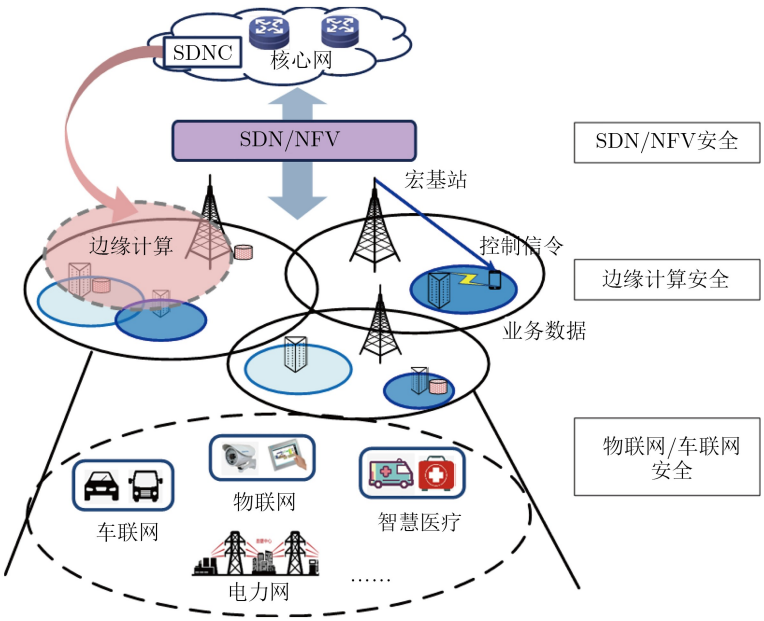



图 1 5G网络架构及新增典型安全需求

安全对抗模型的基础上，对安全对抗进行量化分析，建立安全对抗模型中的相关经济指标，提出新的网络攻防对抗极限计算方法，以衡量网络空间安全的整体安全态势。同时，考虑到5G网络的切片式网络架构可实现对虚拟资源的动态编排，导致网络容量以及网络空间安全对抗极限的动态改变，进而使安全对抗平衡态处于不断建立和被打破的状态，可以研究和分析网络空间安全对抗平衡规律，结合5G网络中边缘计算和SDN集中控制的特点，分析局部攻防平衡与总体攻防平衡的关系，从更加整体化的角度分析5G网络空间安全对抗达到平衡态的规律。

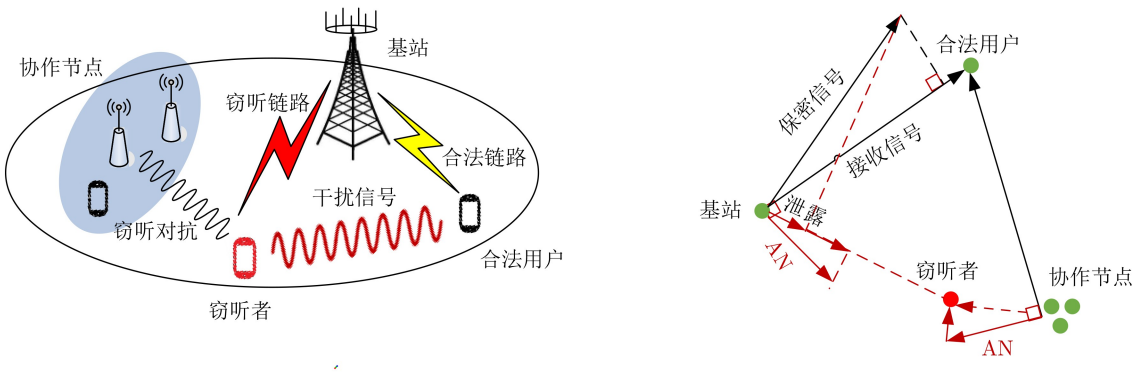
再次，海量物联网(大规模机器类通信)是5G网络的三大应用场景之一，相比于传统网络背景下的网络空间安全对抗，大规模的机器与机器之间的安全对抗将是5G网络空间安全对抗的一大特点。传统网络空间安全攻防对抗面向的“终端”大多为人，在面向人的网络空间安全对抗研究中，人的主观因素和外界影响是决定黑客攻击行为的主要因素，兼具感性和理性于一体的对弈“终端”导致传统网络空间中安全威胁行为和安全对抗行为难以预测。在5G背景下的网络空间兼具海量机器之间的安全对抗，机器的行为是理性、以经济利益最大化为目标的，这为5G网络空间安全中的攻防对抗提供了一定范围内节点行为预测的可能性。因此，可针对海量物联网场景，在对具体攻击行为建模演化的基础上，对攻击单方行为进行预测分析，并通过对其行为规律的系统化研究，实现对网络安全态势整体的感知与调控。

### 3.2 5G网络空间安全对抗博弈模型构建与分析

本节以5G异构融合无线接入网中的安全对抗问题为例，结合物理层安全技术，从宏观的对抗博弈模型构建角度，详细分析无线接入网的窃听对抗和干扰对抗。根据第1节分析，异构融合无线接入网是5G网络的典型接入网结构，由于其具有时空尺度跨度大、网络拓扑频繁变化、通信模式多样化等特点，传统的数据加密、认证等安全机制在异构融合无线接入网中存在处理量增加、协商时延变长、成功协商率下降等问题。物理层安全技术是无线接入网中对抗窃听和干扰的有效技术，通过挖掘无线信道的随机特性可为异构融合无线接入网提供复杂度低、兼容性强的信号安全传输方法，同时5G网络中采用的大规模天线、协同、先进信道编码等物理层技术为物理层安全提供了先天的技术优势。

异构融合无线接入网中多天线系统的窃听与协作窃听对抗以及干扰与干扰对抗问题如图2所示。从窃听角度分析，多天线的主动窃听者通过接收信号的后处理实现对保密信息的最大化窃听，同时，为了破坏合法接收端对保密信息的成功解调，窃听者同时对合法信道(即基站-合法用户信道)发送无线电干扰攻击；从防御角度分析，多天线基站利用天线阵列提供的空间自由度，在发送保密信息的同时向窃听者方向发送人工噪声(Artificial Noise, AN)信号，从而削弱窃听信道(即基站-窃听者信道)对保密信息的窃听质量，此外，为了进一步提升合法信道的保密信号质量，并降低窃听信道的保密信号质量，$J$个协作节点$\mathcal{J}=\{1,2,\cdots,J\}$通过节点选择形成虚拟波束，在合法用户方向发送保密信号，在窃听方向发送干扰噪声。实际系统中，网络节点都是理性且自私的，因此，协作节点一方面辅助基站实现对窃听者的窃听对抗，另一方面，又会根据自己所做的辅助贡献向基站索取“报偿”。这一窃听与协作窃听对抗以及干扰与干扰对抗过程中存在两类博弈问题：基站和协作节点与窃听者之间的对抗博弈，基站与协作节点之间的内部协商博弈。

基站和协作节点与窃听者之间的对抗博弈是非协作博弈，可采用典型的零和博弈模型建立和分析




(a) 多天线系统对抗场景　　(b) 协作窃听对抗矢量示意图

图 2 多天线系统窃听与协作窃听对抗以及干扰与干扰对抗

窃听者与窃听对抗者之间的策略交互，如式(1)和式(2)所示

$$\max_{\boldsymbol{w}_{\mathrm{B}},\boldsymbol{v}_{\mathrm{B}},\phi_{\mathrm{B}},\{\delta_j|j\in\mathcal{J}\},\boldsymbol{w}_{\mathcal{J}},\boldsymbol{v}_{\mathcal{J}}} \max\left(C_{\mathrm{M}}-C_{\mathrm{E}},0\right) \tag{1}$$

$$\min_{\boldsymbol{w}_{\mathrm{E}},\boldsymbol{v}_{\mathrm{E}}} \max\left(C_{\mathrm{M}}-C_{\mathrm{E}},0\right) \tag{2}$$

优化问题式(1)为合法链路的防御目标，即最大化该窃听系统的保密容量，其中$C_{\mathrm{M}}$为合法信道容量，$C_{\mathrm{E}}$为窃听信道容量，其采取的优化策略集合为基站对保密信号和AN信号的预编码向量$\boldsymbol{w}_{\mathrm{B}}$, $\boldsymbol{v}_{\mathrm{B}}$，协作节点的选择策略$\{\delta_j|j\in\mathcal{J}$，如果协作节点$j$被选择，则$\delta_j=1$，否则$\delta_j=0\}$以及所有被选择的协作节点所采取的虚拟天线阵列波束向量$\boldsymbol{w}_{\mathcal{J}}$和$\boldsymbol{v}_{\mathcal{J}}$；优化问题式(2)为窃听者的窃听目标，即最小化该窃听系统的保密容量，其采取的优化策略集合为多接收天线上的信号后处理向量$\boldsymbol{w}_{\mathrm{E}}$以及干扰攻击信号的波束预编码向量$\boldsymbol{v}_{\mathrm{E}}$。

基站与协作节点之间的内部协商博弈可采用斯塔伯克博弈、拍卖模型、联盟博弈等经典博弈模型分析。以斯塔伯克博弈为例，基站作为买方或领导方，其目标为最大化自身的纯收益，如式(3)所示

$$\max_{\boldsymbol{w}_{\mathrm{B}},\boldsymbol{v}_{\mathrm{B}},\phi_{\mathrm{B}},\{P_j|j\in\mathcal{J}\}} \left(\mu_0\max\left(C_{\mathrm{M}}-C_{\mathrm{E}},0\right)-\sum_{j\in\mathcal{J}}\mu_j P_j\right) \tag{3}$$

其中$P_j$是第$j$个协作节点在协助保密信号传输过程中所消耗的资源，$\mu_j$为协作节点对其单位损耗资源的索偿价格，$\mu_0$为窃听系统的单位保密容量收益。因此基站的收益定义为$\mu_0\max\left(C_{\mathrm{M}}-C_{\mathrm{E}},0\right)-\sum_{j\in\mathcal{J}}\mu_j P_j$，即保密信号安全传输的保密容量收益与给予协作节点的报酬之差，也就是基站作为买方的“纯收入”，基站的策略除了自身多天线系统的预编码向量和AN信号功率分配外，与协作节点的交互策略为对协作节点资源的“采购”量。协作节点作为卖方或者跟随方，其优化目标为

$$\max_{\mu_j}\mu_j P_j,\forall j\in\mathcal{J} \tag{4}$$

其中每个协作节点的目标为根据基站对自身资源的“采购”量，以尽可能高的价格$\mu_j$“抛售”损耗资源，即最大化其总收入$\mu_j P_j$。

由优化问题式(1)和式(2)所建立的零和博弈以及优化问题式(3)和式(4)建立的斯塔伯克博弈共同形成了5G异构融合无线接入网中多天线协作系统的窃听干扰混合攻击与对抗博弈数学模型，基于该模型，可进一步分析其中零和博弈和斯塔伯克博弈的均衡态。与此同时，在考虑实际防御系统的资源分配、多天线协作等先进无线技术应用、攻击者攻击策略和攻击能力调整的情况下，可进一步分析该窃听与窃听对抗以及干扰与干扰对抗系统的博弈均衡态的演化趋势。

## 4　结论

5G时代，网络空间的规模和复杂度都远超以往，网络空间安全的影响跨越物理域、逻辑域、社会域和认知域；同时，5G时代的网络攻防将呈现出更加智能化、大规模化、常态化的特点。随着当前5G网络标准和商业部署的推进，从5G网络整体角度研究网络空间安全攻防对抗具有非常重要的研究意义和实际应用价值。如何充分利用网络攻防对抗双方各因素之间的关系和影响力，建立5G网络空间安全对抗博弈模型、探索对抗演化规律以及感知5G安全整体态势，能为网络空间安全攻防领域的研究开拓新的视角。

## 参 考 文 献


[1] International Telecommunications Union. Framework and overall objectives of the future development of IMT for 2020 and beyond[R]. ITU-R, 2015.

[2] CUI Qimei, SHI Yulong, TAO Xiaofeng, *et al*. A unified protocol stack solution for LTE and WLAN in future mobile converged networks[J]. *IEEE Wireless Communications*, 2014, 21(6): 24–33. doi: 10.1109/MWC.2014.7000968.

[3] WU Huici, TAO Xiaofeng, ZHANG Ning, *et al*. Cooperative UAV cluster-assisted terrestrial cellular networks for ubiquitous coverage[J]. *IEEE Journal on Selected Areas in Communications*, 2018, 36(9): 2045–2058. doi: 10.1109/JSAC.2018.2864418.

[4] LORENZ C, HOCK D, SCHERER J, *et al*. An SDN/NFV-enabled enterprise network architecture offering fine-grained security policy enforcement[J]. *IEEE Communications Magazine*, 2017, 55(3): 217–223. doi: 10.1109/MCOM.2017.1600414CM.

[5] ORDONEZ-LUCENA J, AMEIGEIRAS P, LOPEZ D, *et al*. Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges[J]. *IEEE Communications Magazine*, 2017, 55(5): 80–87. doi: 10.1109/MCOM.2017.1600935.

[6] XU Xiaodong, ZHANG Huixin, DAI Xun, *et al*. SDN based next generation mobile network with service slicing and trials[J]. *China Communications*, 2014, 11(2): 65–77. doi: 10.1109/CC.2014.6821738.

[7] 唐伦, 周钰, 杨友超, 等. 5G网络切片场景中基于预测的虚拟网络功能动态部署算法[J]. 电子与信息学报, 2019, 41(9): 2071–2078. doi: 10.11999/JEIT180894.

TANG Lun, ZHOU Yu, YANG Youchao, *et al*. Virtual network function dynamic deployment algorithm based on prediction for 5G network slicing[J]. *Journal of Electronics & Information Technology*, 2019, 41(9): 2071–2078. doi: 10.11999/JEIT180894.

[8] RUPPRECHT D, DABROWSKI A, HOLZ T, *et al*. On security research towards future mobile network generations[J]. *IEEE Communications Surveys & Tutorials*, 2018, 20(3): 2518–2542. doi: 10.1109/COMST.2018.2820728.

[9] DUAN Xiaoyu and WANG Xianbin. Authentication handover and privacy protection in 5G HetNets using software-defined networking[J]. *IEEE Communications Magazine*, 2015, 53(4): 28–35. doi: 10.1109/MCOM.2015.7081072.

[10] LU Xiao, NIYATO D, JIANG Hai, *et al*. Cyber insurance for heterogeneous wireless networks[J]. *IEEE Communications Magazine*, 2018, 56(6): 21–27. doi: 10.1109/MCOM.2018.1700504.

[11] 季新生, 徐水灵, 刘文彦, 等. 一种面向安全的虚拟网络功能动态异构调度方法[J]. 电子与信息学报, 2019, 41(10): 2435–2441. doi: 10.11999/JEIT181130.
JI Xinsheng, XU Shuiling, LIU Wenyan, *et al*. A security-oriented dynamic and heterogeneous scheduling method for virtual network function[J]. *Journal of Electronics & Information Technology*, 2019, 41(10): 2435–2441. doi: 10.11999/JEIT181130.

[12] ITU WP 5D. Minimum requirements related to technical performance for IMT-2020 radio interface(s)[R]. ITU-R, 2017.

[13] 冯登国, 徐静, 兰晓. 5G移动通信网络安全研究[J]. 软件学报, 2018, 29(6): 1813–1825. doi: 10.13328/j.cnki.jos.005547.
FENG Dengguo, XU Jing, and LAN Xiao. Study on 5G mobile communication network security[J]. *Journal of Software*, 2018, 29(6): 1813–1825. doi: 10.13328/j.cnki.jos.005547.

[14] CAO Jin, MA Maode, LI Hui, *et al*. A survey on security aspects for 3GPP 5G networks[J]. *IEEE Communications Surveys & Tutorials*, 2020, 22(1): 170–195. doi: 10.1109/COMST.2019.2951818.

[15] KHAN R, KUMAR P, JAYAKODY D N K, *et al*. A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions[J]. *IEEE Communications Surveys & Tutorials*, 2020, 22(1): 196–248. doi: 10.1109/COMST.2019.2933899.

[16] PONNIAH J, HU Y C, and KUMAR P R. A system-theoretic clean slate approach to provably secure Ad-Hoc wireless networking[J]. *IEEE Transactions on Control of Network Systems*, 2016, 3(2): 206–217. doi: 10.1109/TCNS.2015.2428309.

[17] ALPCAN T and BASAR T. Network Security: A Decision and Game-theoretic Approach[M]. Cambridge: Cambridge University Press, 2010: 37–313.

[18] 杨义先, 钮心忻. 安全通论[M]. 北京: 电子工业出版社, 2018: 39–173.
YANG Yixian and NIU Xinxin. General Theory of Information Security[M]. Beijing: Publishing House of Electronic Industry, 2018: 39–173.

[19] DURKOTA K, LISÝ V, KIEKINTVELD C, *et al*. Case studies of network defense with attack graph games[J]. *IEEE Intelligent Systems*, 2016, 31(5): 24–30. doi: 10.1109/MIS.2016.74.

[20] SANJAB A and SAAD W. Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective[J]. *IEEE Transactions on Smart Grid*, 2016, 7(4): 2038–2049. doi: 10.1109/TSG.2016.2550218.

[21] WANG Kun, YUAN Li, MIYAZAKI T, *et al*. Jamming and eavesdropping defense in green cyber-physical transportation systems using a stackelberg game[J]. *IEEE Transactions on Industrial Informatics*, 2018, 14(9): 4232–4242. doi: 10.1109/TII.2018.2841033.

[22] AHMED I K and FAPOJUWO A O. Stackelberg equilibria of an anti-jamming game in cooperative cognitive radio networks[J]. *IEEE Transactions on Cognitive Communications and Networking*, 2018, 4(1): 121–134. doi: 10.1109/TCCN.2017.2769121.

[23] JIA Luliang, XU Yuhua, SUN Youming, *et al*. Stackelberg game approaches for anti-jamming defence in wireless networks[J]. *IEEE Wireless Communications*, 2018, 25(6): 120–128. doi: 10.1109/MWC.2017.1700363.

[24] LI Yuzhe, SHI Dawei, and CHEN Tongwen. False data injection attacks on networked control systems: A stackelberg game analysis[J]. *IEEE Transactions on Automatic Control*, 2018, 63(10): 3503–3509. doi: 10.1109/TAC.2018.2798817.

[25] HAN Yi, ALPCAN T, CHAN J, *et al*. A game theoretical approach to defend against co-resident attacks in cloud computing: Preventing co-residence using semi-supervised learning[J]. *IEEE Transactions on Information Forensics and Security*, 2016, 11(3): 556–570. doi: 10.1109/TIFS.2015.2505680.

[26] LA Q D, QUEK T Q S, LEE J, *et al*. Deceptive attack and defense game in honeypot-enabled networks for the internet of things[J]. *IEEE Internet of Things Journal*, 2016, 3(6): 1025–2035. doi: 10.1109/JIOT.2016.2547994.

[27] WANG Chunlei, MIAO Qing, and DAI Yiqi. Network survivability analysis based on stochastic game model[C]. The 4th International Conference on Multimedia Information Networking and Security, Nanjing, China, 2014:

199–204. doi: 10.1109/MINES.2012.147.

[28] WEI Longfei, SARWAT A F, SAAD W, *et al*. Stochastic games for power grid protection against coordinated cyber-physical attacks[J]. *IEEE Transactions on Smart Grid*, 2018, 9(2): 684–694. doi: 10.1109/TSG.2016.2561266.

[29] 王元卓, 林闯, 程学旗, 等. 基于随机博弈模型的网络攻防量化分析方法[J]. 计算机学报, 2010, 33(9): 1748–1762. doi: 10.3724/SP.J.1016.2010.01748.
WANG Yuanzhuo, LIN Chuang, CHENG Xueqi, *et al*. Analysis for network attack-defense based on stochastic game model[J]. *Chinese Journal of Computers*, 2010, 33(9): 1748–1762. doi: 10.3724/SP.J.1016.2010.01748.

[30] DORASZELSKI U and ESCOBAR J F. A theory of regular markov perfect equilibria in dynamic stochastic games: Genericity, stability, and purification[J]. *Theoretical Economics*, 2010, 5(2): 369–402. doi: 10.3982/TE632.

[31] XIAO Liang, XU Dongjin, XIE Caixia, *et al*. Cloud storage defense against advanced persistent threats: A prospect theoretic study[J]. *IEEE Journal on Selected Areas in Communications*, 2017, 35(3): 534–544. doi: 10.1109/JSAC.2017.2659418.

[32] ZHANG Rui, ZHU Quanyan, and HAYEL Y. A Bi-level game approach to attack-aware cyber insurance of computer networks[J]. *IEEE Journal on Selected Areas in Communications*, 2017, 35(3): 779–794. doi: 10.1109/JSAC.2017.2672378.

[33] MIN Minghui, XIAO Liang, XIE Caixia, *et al*. Defense against advanced persistent threats in dynamic cloud storage: A colonel blotto game approach[J]. *IEEE Internet of Things Journal*, 2018, 5(6): 4250–4261. doi: 10.1109/JIOT.2018.2844878.

[34] LASZKA A, HORVATH G, FELEGYHAZI M, *et al*. FlipThem: Modeling Targeted Attacks with Flipit for Multiple Resources[M]. POOVENDRAN R and SAAD W. Decision and Game Theory for Security. Cham: Springer, 2014: 175–194. doi: 10.1007/978-3-319-12601-2_10.

[35] WANG Chong, HOU Yunhe, and TEN C W. Determination of Nash equilibrium based on plausible attack-defense dynamics[J]. *IEEE Transactions on Power Systems*, 2017, 32(5): 3670–3680. doi: 10.1109/TPWRS.2016.2635156.

[36] HUANG Shirui, ZHANG Hengwei, WANG Jindong, *et al*. Markov differential game for network defense decision-making method[J]. *IEEE Access*, 2018, 6: 39621–39634. doi: 10.1109/ACCESS.2018.2848242.

[37] ZHANG Hengwei, JIANG Lü, HUANG Shirui, *et al*. Attack-defense differential game model for network defense strategy selection[J], *IEEE Access*, 2018, 7: 50618–50629. doi: 10.1109/ACCESS.2018.2880214.

[38] GARCIA E, CASBEER D W, and PACHTER M. Design and analysis of state-feedback optimal strategies for the differential game of active defense[J]. *IEEE Transactions on Automatic Control*, 2019, 64(2): 553–568. doi: 10.1109/TAC.2018.2828088.

[39] SHEN Shigen, LI Yuanjie, XU Hongyun, *et al*. Signaling game based strategy of intrusion detection in wireless sensor networks[J]. *Computers & Mathematics with Applications*, 2011, 62(6): 2404–2416. doi: 10.1016/j.camwa.2011.07.027.

[40] MALEKI H, VALIZADEH S, KOCH W, *et al*. Markov modeling of moving target defense games[C]. The 2016 ACM Workshop on Moving Target Defense, Vienna, Austria, 2016: 81–92. doi: 10.1145/2995272.2995273.

[41] LEI Cheng, MA Duohe, and ZHANG Hongqi. Optimal strategy selection for moving target defense based on Markov game[J]. *IEEE Access*, 2017, 5: 156–169. doi: 10.1109/ACCESS.2016.2633983.

[42] SEDJELMACI S A H, BRAHMI I H, ANSARI N, *et al*. Cyber security framework for vehicular network based on a hierarchical game[J]. *IEEE Transactions on Emerging Topics in Computing*, 2019. doi: 10.1109/TETC.2018.2890476.

[43] BALKENBORG D and SCHLAG K H. On the interpretation of evolutionary stable sets in symmetric and asymmetric games[R]. Mimeo, Bonn University Economics Department, 1994.

[44] FIONDELLA L, RAHMAN A, LOWNES N, *et al*. Defense of high-speed rail with an evolutionary algorithm guided by game theory[J]. *IEEE Transactions on Reliability*, 2016, 65(2): 674–686. doi: 10.1109/TR.2015.2491602.

[45] HU Hao, LIU Yuling, ZHANG Hongqi, *et al*. Optimal network defense strategy selection based on incomplete information evolutionary game[J]. *IEEE Access*, 2018, 6: 29806–29821. doi: 10.1109/ACCESS.2018.2841885.

[46] HUANG Jianming, ZHANG Hengwei, and WANG Jindong. Markov evolutionary games for network defense strategy selection[J]. *IEEE Access*, 2017, 5: 19505–19516. doi: 10.1109/ACCESS.2017.2753278.

[47] MIEHLING E, RASOULI M, and TENEKETZIS D. Optimal defense policies for partially observable spreading processes on Bayesian attack graphs[C]. The 2nd ACM Workshop on Moving Target Defense, Colorado, USA, 2015: 67–76.

[48] 陈小军, 方滨兴, 谭庆丰, 等. 基于概率攻击图的内部攻击意图推断算法研究[J]. 计算机学报, 2014, 37(1): 62–72.
CHEN Xiaojun, FANG Binxing, TAN Qingfeng, *et al*. Inferring attack intent of malicious insider based on probabilistic attack graph model[J]. *Chinese Journal of Computers*, 2014, 37(1): 62–72.

[49] FUDENBERG D and TIROLE J. Game Theory[M].

Cambridge: Massachusetts Institute of Technology Press, 1991: 65–203.

[50] ABASS A A A, XIAO Liang, MANDAYAM N B, *et al*. Evolutionary game theoretic analysis of advanced persistent threats against cloud storage[J]. *IEEE Access*, 2017, 5: 8482–8491. doi: 10.1109/ACCESS.2017.2691326.

[51] BHARATHI S, KUMAR D, and RAM D. Defence against responsive and non-responsive jamming attack in cognitive radio networks: An evolutionary game theoretical approach[J]. *The Journal of Engineering*, 2018, 2018(2): 68–75. doi: 10.1049/joe.2017.0285.

[52] HAN Zhu, MARINA N, DEBBAH M, *et al*. Physical layer security game: How to date a girl with her boyfriend on the same table[C]. The 1st ICST International Conference on Game Theory for Networks, Istanbul, Turkey, 2009: 287–294. doi: 10.1109/GAMENETS.2009.5137412.

[53] ZHANG Rongqing, SONG Lingyang, HAN Zhu, *et al*. Physical layer security for two-way untrusted relaying with friendly jammers[J]. *IEEE Transactions on Vehicular Technology*, 2012, 61(8): 3693–3704. doi: 10.1109/TVT.2012.2209692.

[54] CHU Zheng, CUMANAN K, DING Zhiguo, *et al*. Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer[J]. *IEEE Transactions on Vehicular Technology*, 2015, 64(5): 1833–1847. doi: 10.1109/TVT.2014.2336092.

[55] WU Huici, TAO Xiaofeng, HAN Zhu, *et al*. Secure transmission in MISOME wiretap channel with multiple assisting jammers: Maximum secrecy rate and optimal power allocation[J]. *IEEE Transactions on Communications*, 2017, 65(2): 775–789. doi: 10.1109/TCOMM.2016.2636288.

[56] FANG He, XU Li, and WANG Xianbin. Coordinated multiple-relays based physical-layer security improvement: A single-leader multiple-followers stackelberg game scheme[J]. *IEEE Transactions on Information Forensics and Security*, 2018, 13(1): 197–209. doi: 10.1109/TIFS.2017.2746001.

[57] FANG He, XU Li, ZOU Yulong, *et al*. Three-stage stackelberg game for defending against full-duplex active eavesdropping attacks in cooperative communication[J]. *IEEE Transactions on Vehicular Technology*, 2018, 67(11): 10788–10799. doi: 10.1109/TVT.2018.2868900.

[58] WANG Wei, TEH K C, LI K H, *et al*. On the impact of adaptive eavesdroppers in multi-antenna cellular networks[J]. *IEEE Transactions on Information Forensics and Security*, 2018, 13(2): 269–279. doi: 10.1109/TIFS.2017.2746010.

[59] LUO Yijie, FENG Zhibin, JIANG Han, *et al*. Game-theoretic learning approaches for secure D2D communications against full-duplex active eavesdropper[J]. *IEEE Access*, 2019, 7: 41324–41335. doi: 10.1109/ACCESS.2019.2906845.

[60] LI Meng, ZHANG Yanru, WANG Li, *et al*. Incentive design for collaborative jamming using contract theory in physical layer security[C]. 2016 IEEE/CIC International Conference on Communications in China, Chengdu, China, 2016: 1–6, doi: 10.1109/ICCChina.2016.7636873.

[61] HAN Zhu, MARINA N, DEBBAH M, *et al*. Improved wireless secrecy rate using distributed auction theory[C]. The 5th International Conference on Mobile Ad-hoc and Sensor Networks, Fujian, China, 2009: 442–447. doi: 10.1109/MSN.2009.73.

[62] ZHANG Rongqing, SONG Lingyang, HAN Zhu, *et al*. Improve physical layer security in cooperative wireless network using distributed auction games[C]. 2011 IEEE Conference on Computer Communications Workshops, Shanghai, China, 2011: 18–23. doi: 10.1109/INFCOMW.2011.5928805.

[63] KHAN A S, RAHULAMATHAVAN Y, BASUTLI B, *et al*. Blockchain-based distributive auction for relay-assisted secure communications[J]. *IEEE Access*, 2019, 7: 95555–95568. doi: 10.1109/ACCESS.2019.2929136.

[64] SAAD W, HAN Zhu, BASAR T, *et al*. Physical layer security: Coalitional games for distributed cooperation[C]. The 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, Seoul, South Korea, 2009: 1–8.

[65] WANG Kun, YUAN Li, MIYAZAKI T, *et al*. Strategic antieavesdropping game for physical layer security in wireless cooperative networks[J]. *IEEE Transactions on Vehicular Technology*, 2017, 66(10): 9448–9457. doi: 10.1109/TVT.2017.2703305.

[66] WANG Kun, YUAN Li, MIYAZAKI T, *et al*. Antieavesdropping with selfish jamming in wireless networks: A Bertrand game approach[J]. *IEEE Transactions on Vehicular Technology*, 2017, 66(7): 6268–6279. doi: 10.1109/TVT.2016.2639827.

[67] YUKSEL M, LIU Xi, and ERKIP E. A secure communication game with a relay helping the eavesdropper[J]. *IEEE Transactions on Information Forensics and Security*, 2011, 6(3): 818–830. doi: 10.1109/TIFS.2011.2125956.

[68] ALSABA Y, LEOW C Y, and ABDUL RAHIM S K. A zero-sum game approach for non-orthogonal multiple access systems: Legitimate eavesdropper case[J]. *IEEE Access*, 2018, 6: 58764–58773. doi: 10.1109/ACCESS.2018.2874215.

[69] SAGDUYU Y E, BERRY R, and EPHREMIDES A. MAC

games for distributed wireless network security with incomplete information of selfish and malicious user types[C]. The 2009 International Conference on Game Theory for Networks, Istanbul, Turkey, 2009: 130–139. doi: 10.1109/GAMENETS.2009.5137394.

[70] TANG Ling, CHEN Hao, and LI Qianmu. Social tie based cooperative jamming for physical layer security[J]. *IEEE Communications Letters*, 2015, 19(10): 1790–1793. doi: 10.1109/LCOMM.2015.2462826.

[71] LÜ Shichao, XIAO Liang, HU Qing, *et al*. Anti-jamming power control game in unmanned aerial vehicle networks[C]. 2017 IEEE Global Communications Conference, Singapore, 2017: 1–6. doi: 10.1109/GLOCOM.2017.8253988.

[72] LU Xiaozhen, XU Dongjin, XIAO Liang, *et al*. Anti-jamming communication game for UAV-aided VANETs[C]. 2017 IEEE Global Communications Conference, Singapore, 2017: 1–6. doi: 10.1109/GLOCOM.2017.8253987.

徐　璟：女，1981年生，副教授，研究方向为宽带移动通信、无线网络安全.

吴慧慈：女，1992年生，助理教授，研究方向为无线接入安全、异构融合协作.

陶小峰：男，1970年生，教授，博士生导师，研究方向为无线通信、移动通信安全.

责任编辑：余　蓉