无人机协同传输通信系统物理层安全技术研究*

张倩倩

（南京审计大学金审学院 信息科学与工程学院，江苏 南京 210046）

摘　要：针对无人机中继系统中存在窃听节点的问题，研究了采用信源端发送人工干扰信号的方式来提高系统的安全容量。仿真结果表明，在无人机中继系统中，由于无人机自身的特性及人工干扰的影响，比传统采用固定中继形式具有更好的安全容量，并且在信源端发送信号功率一定的条件下，该系统具有最佳功率分配方案。

关键词：无人机中继；窃听节点；人工干扰；安全容量；功率分配

中图分类号：TP391　　**文献标识码**：A　　DOI：10.19358/j.issn.2096-5133.2020.05.007

引用格式：张倩倩. 无人机协同传输通信系统物理层安全技术研究[J]. 信息技术与网络安全，2020，39(5)：33-36.

Research on physical layer security technology in UAV cooperative transmission communication system

Zhang Qianqian

（School of Information Science and Engineering，Nanjing Audit University Jinshen College，Nanjing 210046，China）

Abstract：Aiming at the problem of eavesdropping node in UAV relay system，the method of sending artificial interference signal from the source is studied to improve the security capacity of the system. The simulation results show that the UAV relay system has better security capacity than the traditional fixed relay system because of the characteristics of the UAV and the influence of artificial interference. Moreover，the system has the optimal power distribution scheme under the condition that the signal power at the source is certain.

Key words：UAV relay；eavesdropping node；artificial interference；security capacity；power allocation

0　引言

作为一种分布式的虚拟多天线传输技术，协同传输通信技术融合了分集与中继传输的技术优势，在不增加天线的基础上，可在传统网络中实现并获得多天线与多跳传输的性能增益，从而提高系统的传输性能，带来了无线通信领域的巨大变革[1]。对任何通信系统而言，信息传输的安全性、可靠性、有效性同等重要，都直接决定着系统的可用性。而在协同传输通信系统中，采用中继节点进行信息的协同传输虽然提高了信息传输的可靠性和有效性，但却使信息传输面临着严重的安全威胁。因为无线信道的开放性可使信号传播范围内的所有接收机均有可能接收到发射信号，给无线通信带来了严重的安全威胁，而且协同传输系统中中继节点的介入会使得系统子信道数大为增加，这样系统中传输的信息更容易被他人窃听。

在传统的陆地无线通信系统中，文献[2-5]提出中继协同技术能有效扩大无线网络的覆盖范围，并提高无线系统的物理层安全容量。文献[6-8]利用中继协同技术提高了无线通信系统的安全容量，相比于传统的直传链路和轮回调度方法，显著增强了无线通信系统的安全性。文献[9-10]联合考虑了中继与干扰技术，通过增加人工干扰进一步改善了无线传输的保密性。此外，物理层安全技术利用无线信道特性可以实现轻量级的安全加密，近年来也引起了广泛的研究兴趣。文献[11]验证了在传感器网络中可以利用物理层安全技术实现可靠通信。文献[12]分析了引入协作干扰后传感器网络的安全性能，并且推导出安全容量的闭式表示。当网络为双向中继网络时，文献[13]提出了一种最优的能量分配方式以最大化网络总的安全速率。针对射频无线充能的多天线传感器网络，文献[14]提出了

* 基金项目：江苏省高等学校自然科学基金项目(19KJD120001)

www.pcachina.com

一个两阶段的安全传输协议,通过对发送功率、信息波束成型等参数进行联合优化以提高网络的安全能量效率。

然而,传统思维陆地通信系统物理层安全中,通常采用固定式的或者准静态的中继节点,因此无线通信的物理层安全中中继节点的位置对合法链路的链路质量具有较大的影响。此外,在一些特殊的场景中,例如战场上,战场态势是不断变化的,采用固定的中继节点很显然不能满足特殊的需求。近年来,由于无人机具有多种优势,例如高速移动性、低成本、按需部署等,无人机在无线通信中得到广泛使用。现有的无人机协作通信在提高物理层安全方面主要通过博弈建模[15-16]、功资源管理[17-18]、轨迹优化[19-20]等方式。

本文主要研究了无人机作为中继节点的协同传输通信系统。在源节点、目的节点与窃听节点位置固定的前提下,充当中继的无人机在源节点与目的节点之间来回飞行,可以减小信息接收与中继转发阶段的信息传输距离,进而降低信息传输过程中的大尺度损耗。对于窃听节点,无人机中继的运动是随机的,因此相比于主信道,窃听信道容量不能获得相应的改善,从而有效提高了无人机中继系统的安全容量。此外,在信息传输中,通过在源节点加入人工干扰噪声的方式减少额外噪声节点给网络带来的开销。文中通过与采用固定中继节点的对比得出采用无人机中继的方式能有效提高系统的安全容量。此外,在信源端发送功率一定的条件下存在最佳功率分配方案,可使系统安全容量达到最大值。

1 系统模型

系统模型如图 1 所示。为简便起见,这里假设两信源之间没有直接通路,只能通过中继节点进行信息协同传输,并且假设窃听节点为了防止被侦察到,窃听节点位于源节点与目的节点中间的位置。此外,由于本文只对无人机中继做初步的探讨,文中暂时不考虑无人机飞行中信道的快衰落与多普勒效应。图 1 中 S 为信源节点,D 为目的节点,U 为中继节点,E 为窃听节点。用 x_S、x_J 分别表示信源 S 发送的有用信号及干扰信号;源节点发送的信号总功率为 E_0($E_0 = E_S + E_J$,E_S 为有用信号功率,E_J 为干扰信号功率);源节点到无人机的信道系数为 h_{SU},源节点到窃听节点的信道系数为 h_{SE},无人机节点到目的节点的信道系数为 h_{UD}。

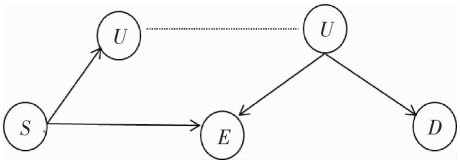

图 1 系统框图

图 1 所示的无人机协同传输系统模型中,信息传输分为两个阶段。第一个阶段,源节点将信息及干扰信号发送给无人机节点,此时无人机节点、窃听节点均能同时接收到源节点的信号,信号公式分别如式(1)、(2)所示。

$$y_U = n_{SU} + \sqrt{E}(x_S + x_J)h_{SU} \tag{1}$$

$$y_E = n_{SE} + \sqrt{E}(x_S + x_J)h_{SE} \tag{2}$$

式中,n_{SU}、n_{SD} 分别表示无人机节点与窃听节点处的信道噪声,均可被建模为均值为 0、方差为 σ^2 的高斯随机变量。在这一阶段,外在恶意窃听节点窃听到的信道容量如式(3)所示。

$$C_{E_1} = \frac{W}{2}\log_2\left(1 + \frac{E_S|h_{SE}|^2}{\sigma^2 + E_J|h_{SE}|^2}\right) \tag{3}$$

式中,W 表示带宽。

无人机接收到的信道容量如式(4)所示。

$$C_U = \frac{W}{2}\log_2\left(1 + \frac{E_S|h_{SU}|^2}{\sigma^2 + E_J|h_{SU}|^2}\right) \tag{4}$$

第二阶段,无人机节点将接收的信号 y_u 经过一段时间的飞行,在距离目的节点一定的位置将信号放大转发给目地节点,发送功率为 E_U,放大系数 β 如式(5)所示。

$$\beta = \sqrt{\frac{E_U}{E_S|h_{SU}|^2 + E_J|h_{JU}|^2 + \sigma^2}} \tag{5}$$

相应的 D 接收到的信号 y_D 如式(6)所示。

$$y_D = \beta\sqrt{E_U}h_{UD}y_U + n_{UD} \tag{6}$$

外在恶意窃听节点 E 接收到的信号 y_{E_2} 如式(7)所示。

$$y_{E_2} = \beta\sqrt{E_U}h_{UE}y_U + n_{UE} \tag{7}$$

需要注意,本文设计的模型中干扰信号是在源节点加入的,在中间传输过程中干扰信号一直存在,对于目的节点来说干扰信号是已知的,因此目的节点滤除干扰信号就可以得到应该要接收的信号,D 接收到的信号以及 U 到 D 的信噪比分别为式(8)、式(9)所示。

www.bcachina.com

$$\tilde{y}_D = \chi x_S + \omega \tag{8}$$

其中，$\chi = \beta\sqrt{E_U E_S h_{UD}}\omega = \beta n_{SU}\sqrt{E_U h_{UD}} + n_{UD}$。

$$\gamma_D = \frac{E_U|h_{UD}|^2}{\sigma^2 + K + \dfrac{\sigma^2|h_{JD}|^2}{E_U|h_{UD}|^2}E_J} \tag{9}$$

式中，$K = (\sigma^2(E_U|h_{UD}|^2 + \sigma^2)/E_U|h_{UD}|^2)$。

根据山农信道容量公式，双向中继信道中，信源与目的节点之间的信道容量 C_D 如式(10)所示。

$$C_D = \frac{W}{2}\log_2(1 + \gamma_D) \tag{10}$$

此外，第二阶段窃听节点窃听到的信道容量如式(11)所示。

$$C_{E_2} = \frac{W}{2}\log_2\left(1 + \frac{E_U|h_{UE}|^2}{\sigma^2 + E_J|h_{UE}|^2}\right) \tag{11}$$

2 系统安全性能分析

本文使用安全容量这一性能对系统的安全性能进行分析。根据 Wyner 对安全容量的定义，本系统安全容量可以表示为：

$$C_S = (C_U + C_D - C_{E_1} - C_{E_2})^+ \tag{12}$$

其中，$(x)^+$ 表示$\{x,0\}$中的最大值。

本文所述邪恶系统模型中，是通过在信源端加入人为干扰噪声的方式来增强系统信息传输的安全性的。因此，干扰信号的设置将影响整个系统的安全性能的获取，是系统实现安全通信的关键。为实现安全通信，应有：

$$\max C_S = \max(C_U + C_D - C_{E_1} - C_{E_2})$$
$$\text{s.t.}\begin{cases} C_U + C_D \geqslant C_{E_1} + C_{E_2} \\ 0 \leqslant E_S, E_J, E_U \leqslant E_{\max} \end{cases} \tag{13}$$

式中，$E_{\max}$ 为系统最大传输功率。

3 系统仿真与分析

3.1 场景 A

若系统中，信源节点发送的信号的总功率一定，假设有用信号与噪声信号功率相同，则在分析中将重点分析信道衰落对系统安全性能的影响。

假设噪声方差 $\sigma^2 = 1$，传输带宽 $W = 1$，有用信号功率与噪声信号功率相同 $E_S = E_J$，分别采用无人机中继与固定节点中继方式。从图 2 中可以看出在整个信噪比范围内，采用无人机中继比采用固定节点中继方式具有更高的安全容量，系统安全性能更好。

3.2 场景 B

若系统中，信源节点发送的信号总功率一定，

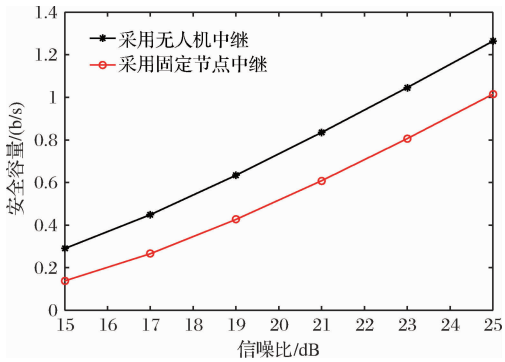

图 2 不同中继方式下安全容量对比图

但有用信号功率与噪声信号功率不相同，则此时存在最佳功率分配问题。

在许多实际系统中系统总的发送功率通常是有一定限制的。也就是说，在系统总发送功率受限条件下对上述问题进行讨论将具有更大的实用价值。现假设系统总发送功率一定且为 E_0，干扰信号占系统总功率的比例为 a，即 $E_J = aE_0$。从图 3 中可以看出：(1)当系统总发送功率一定时，随着干扰信号功率占比的增加，系统安全容量曲线呈现先逐渐升高再逐渐降低的趋势；(2)当干扰信号功率占总功率比例在 0.4 时，即 $a = 0.4$ 时系统可获得最大安全容量。

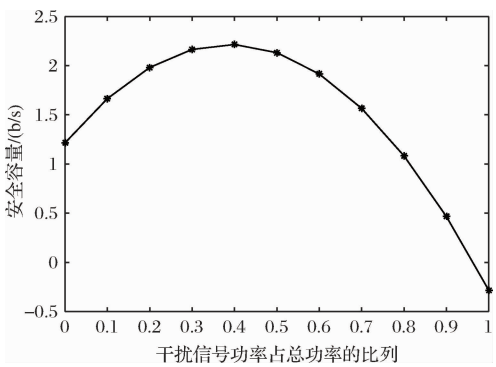

图 3 采用无人机中继时最佳功率分配

4 结论

本文对无人机在协同传输通信中的应用进行了初步的讨论，系统假设存在窃听节点的前提下，采用信源节点发送有用信号与人工噪声的方式进行通信，通过对比采用无人机中继与固定节点中继的结果得出，采用无人机中继能够得到较好的系统性能，无人机中继可在很多特殊的场景下使用，因此具有较好的前景。在此基础上，本文分析了采用无人机中继时，系统功率分配的问题。在发送信号

www.pcachina.com

总功率一定的条件下,有用信号功率与噪声功率所占比例对系统安全性能具有一定的影响。通过利用无人机本身的特性和在信源端发送人工干扰的方式可以提高系统的安全性能。

参考文献

[1] 臧国珍,王恺,夏莹. 基于 Alamouti 码的卫星差分协同方案设计与仿真[J]. 军事通信技术,2011,32(3):1-6.

[2] DONG L, HAN Z, PETROPULU A, et al. Secure wireless communications via cooperation[C]. Chicago: Speech and Signal Processing,2008.

[3] DONG L, HAN Z, PETROPULU A, et al. Amplify-and-forward based cooperation for secure wireless communications [C]. Taiwan China: Speech and Signal Processing,2009.

[4] DONG L, HAN Z, PETROPULU A, et al. Cooperative jamming for wireless physical layer security[C]. Taiwan China: Speech and Signal Processing,2009.

[5] DONG L, HAN Z, PETROPULU A, et al. Improving wireless physical layer security via cooperating relays[J]. IEEE Transactions on Signal Processing,2010,58:1875-1888.

[6] ZOU Y L, WANG X B, SHEN W M. Optimalrelay selection for physical_layer security in cooperativewireless networks [J]. IEEE Journal on Selected Areas in Communications, 2013,31:2099-2111.

[7] DING X J, SONG T C, ZOU Y L, et al. Relay selection for secrecy improvement in cognitive amplify-and-forward relay networks against multiple eavesdroppers[J]. IET Communications,2016,10:2043-2053.

[8] ZOU Y L, CHAMPAGNE B, ZHU W P, et al. Relay-selection improves the security reliability trade-off in cognitive radio systems[J]. IEEE Transactions on Communications, 2015,63:215-228.

[9] HUI H, SWINDLEHURST A L, LI G B, et al. Secure relay and jammer selection for physical layer security[J]. IEEE Signal Processing Letters,2015,22:1147-1151.

[10] WANG L, CAI Y, ZOU Y, et al. Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays[J]. IEEE Transactions on Vehicular Technology,2016,65:6259-6274.

[11] EHRLIC M, WISNIEWSK L, JASPERNEITE J. State of the art and future applications of industrial wireless sensor networks[C]. Berlin: Kommunikationund bildverarbeitung in derautomation,2018.

[12] MAMAGHANI M T, KUHESTANI A, WONG K K. Secure twoway transmission via wireless- powered untrusted relay and external jammer[J]. IEEE Transactions on Vehicular Technology,2018,67:8451- 8465.

[13] KUHESTANI A, MOHAMMADI, YEOH P L. Optimal power allocation and secrecy sum rate in two-way untrusted relaying networks with an external jammer[J]. IEEE Transactionson Communications,2018,66:2671- 2684.

[14] 刘笑辰,高媛媛,系和平. 安全能量效率优化的传感器网络传输研究[J]. 计算机工程与应用,2019,55(21):122-128.

[15] BHATTACHARYYA S, BAAR T. Game-theoretic analysis of an aerial jamming attack on a UAV communication network[C]. USA: American Control Conference,2010.

[16] XIA C X, XIAO L. User-centric view of smart attacks in wireless networks[C]. Nanjing: ICUWB,2016.

[17] SHARAWI M S, ALOI D N, RAWASHDEH O A, et al. Design and implementation of embedded printed antenna arrays in small UAV wing structures[J]. EEE Transactions on Antennas and Propagation,2010,58:2531-2538.

[18] ZHANG G, WU Q, CUI M. Securing UAV communications via trajectory optimization[J]. IEEE Globecom, 2017,67:1-6.

[19] WU Q, XU J, ZHANG R. Capacity characterization of UAV-enabled two-user broadcast channe[J]. IEEE Journal on Selected Areas in Communications,2018,23:1-6.

[20] WU Q, ZHANG R. Common throughput maximization in UAV-enabled OFDMA systems with delay consideration[J]. IEEE Transactions on Communications,2018,2:147-152.

(收稿日期:2020-03-18)

作者简介:

张倩倩(1989 -),女,硕士研究生,助教,主要研究方向:网络空间安全。

www.pcachina.com

版权声明

经作者授权，本论文版权和信息网络传播权归属于《信息技术与网络安全》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《信息技术与网络安全》编辑部

中国电子信息产业集团有限公司第六研究所