

车联网中基于攻防博弈的蜜罐防御及传输策略

易杰¹, 曹腾飞¹, 郜帅², 黄建强¹

(1. 青海大学计算机技术与应用系, 青海 西宁 810016; 2. 北京交通大学移动专用网络国家工程研究中心, 北京 100044)

摘要: 随着车联网的快速发展, 服务提供商通过将 5G 基站型路侧单元 (RSU, road side unit) 部署在靠近车辆的位置, 能够迅速为车辆用户提供缓存服务。然而, 由于恶意攻击者的存在, 其通过控制基站获取权限使基站变为恶意基站, 达到身份伪造攻击的目的, 并以恶意基站的名义发送消息干扰车辆与可信基站之间的通信链路, 容易造成严重的行车安全问题。提出了车联网中基于攻防博弈的蜜罐防御及传输策略, 通过部署蜜罐基站混淆攻击者, 从而降低车联网中身份伪造攻击的风险, 提高车联网数据传输的可靠性。将车联网场景中可信基站与恶意基站之间的交互问题建模为攻防博弈模型, 在此基础上可信基站与蜜罐基站联合作为防守方来抵御恶意攻击。可信基站和恶意基站作为攻防博弈双方选择各自相应的策略, 构建双方效益函数模型, 并结合车辆时延反馈机制, 防守方与恶意基站动态调整各自策略。通过调整蜜罐基站与车辆的交互性和 IP 随机化程度, 使防守方的整体效益得到有效提升, 并利用混合策略纳什均衡理论得出最优解。大量的仿真实验结果表明, 所提出的策略能够在恶意攻击者存在的情况下, 提高车联网服务的安全传输性能, 对比无蜜罐防御方案, 防守方期望效益提升了 48.9%, 数据传输时延降低了 57.1%。

关键词: 车联网; 博弈论; 蜜罐策略; 攻防博弈

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022050

Honeypot defense and transmission strategy based on offensive and defensive games in vehicular networks

YI Jie¹, CAO Tengfei¹, GAO Shuai², HUANG Jianqiang¹

1. Department of Computer Technology and Applications, Qinghai University, Xining 810016, China

2. National Engineering Research Center for Mobile Private Networks, Beijing Jiaotong University, Beijing 100044, China

Abstract: With the rapid development of the Internet of Vehicles, service providers can efficiently provide caching

收稿日期: 2022-01-20; 修回日期: 2022-05-11

通信作者: 曹腾飞, caotf@qhu.edu.cn

基金项目: 国家自然科学基金 (62101299, 62162053); 青海省自然科学基金 (2020-ZJ-943Q)

Foundation Items: The National Natural Science Foundation of China (62101299, 62162053), The Natural Science Foundation of Qinghai Province (2020-ZJ-943Q)

引用格式: 易杰, 曹腾飞, 郜帅, 等. 车联网中基于攻防博弈的蜜罐防御及传输策略[J]. 网络与信息安全学报, 2022, 8(4): 157-167.

Citation Format: YI J, CAO T F, GAO S. Honeypot defense and transmission strategy based on offensive and defensive games in vehicular networks[J]. Chinese Journal of Network and Information Security, 2022, 8(4): 157-167.

services for vehicle users by deploying 5G base station-type RSUs adjacent to vehicles. However, due to the presence of malicious attackers, the controlled base station is turned to be malicious for the purpose of identity forgery attack. When messages are sent in the name of malicious base stations to interfere with the communication link between vehicles and the trusted base stations, it is easy to cause serious driving safety problems. To solve the above problem, an efficient transmission and honeypot defense strategy was proposed, which was based on the offensive and defensive game in the Internet of Vehicles to reduce the risk of identity forgery attacks and improve the security of data transmission. The interaction between trusted base stations and malicious base stations in the Internet of Vehicles scenario was modeled as an attack-defense game model. On this basis, trusted base stations and honeypot base stations were jointly used as defenders to defend against malicious attacks. Then, the trusted base station and the malicious base station, as the two sides of the offensive and defensive game, chose their respective strategies to construct a model of the benefit function of both sides. Combined with the vehicle delay feedback mechanism, the defender and the malicious base station dynamically adjusted their respective strategies. By adjusting the interaction between the honeypot base station and the vehicle, and also the degree of IP randomization, the overall benefit of the defender was effectively improved. Besides, the optimal solution was obtained by using the mixed strategy Nash equilibrium theory. Simulation experimental results show that the proposed strategy can improve the secure transmission performance of the Internet of Vehicles service in the presence of malicious attackers, and the defender's expected benefit is improved by 48.9% and the data transmission delay is reduced by 57.1% compared to the no-honeypot defense scheme.

Keywords: Internet of vehicles, game theory, honeypot strategy, offensive and defensive games

0 引言

随着 5G、物联网、人工智能等技术日趋成熟,智慧交通逐渐兴起。车联网作为一种新型的智慧交通系统,可以实现人、车、路、云、网、环境等交通参与物理要素的连接。5G 通信技术可以提供低时延、高带宽和广连接的服务,大大促进了现实场景下车联网技术的发展与应用。根据车联网产业报告^[1],我国车联网产业进入高速发展阶段,现有机动车保有量约为 3.95 亿辆,汽车保有量突破 3 亿,未来智能网联汽车将继续增长达到 7 800 万辆,这样庞大的汽车市场为车联网技术和服

务的发展带来了可能。在车联网应用的过程中,将产生大量的移动数据流量,在数据传输过程中受到恶意攻击的风险日益增加,导致车内敏感信息泄露或被篡改,引起车辆行驶的混乱,还有可能危及人的生命安全。因此,车联网面临的安全形势严重,如何提高车联网的数据安全传输具有重要的意义。

让车辆失控引发交通事故,更有攻击者可轻松伪造红绿灯交通信息,控制无人驾驶车辆违背交通信号行驶,影响驾驶安全。在车联网中存在的身份伪造攻击是攻击者以其他车辆或 RSU 的名义发送消息,本文针对身份伪造攻击问题,引入蜜罐欺骗防御策略减少车联网中 RSU 被恶意控制的风险。蜜罐欺骗是一种主动欺骗防御技术^[2],它的优势是通过部署轻量级安全资源,诱导攻击者进行攻击,减少攻击者对网络中关键资源的威胁,提升网络系统的安全性能,同时部署蜜罐所需的开发和计算资源成本较低,因此综合考虑在车联网中部署蜜罐基站是可行的。

基于以上车联网安全风险以及蜜罐防御策略的分析,无线通信链路被恶意干扰的风险增大,在车联网中对无线网络通信的安全性、可靠性以及稳定性要求更高。同时,随着智能车辆的快速发展和更新,联网的车辆将产生大量数据,车联网将成为关键数据节点和数据中心,用户对安全性强的车辆网络应用以及高质量的服务需求逐渐提高。因此,车联网信息安全至关重要,如何减小被攻击者攻击的概率并且降低数据传输时延,提高用户的服务体验质量,是当前亟待解决的问

题。为了减少车联网在数据传输过程中受到恶意干扰的风险,本文基于攻防博弈理论,对车联网中可信基站的数据安全传输问题进行了研究,主要针对的攻击方式是身份伪造攻击。本文引入网络欺骗技术,将可信基站和蜜罐基站作为防守方,蜜罐基站通过欺骗策略从而混淆攻击者,提高攻击者成本。利用混合纳什均衡得到攻防博弈的唯一纳什均衡解,并且通过车联网数据传输时延作为反馈评价,进一步动态调整蜜罐基站的欺骗策略,在保证传输时延较低的情况下,提高可信基站的收益。本文的主要贡献包括以下几点。

1) 在车联网系统中,引入攻防博弈,分析防守方和攻击方各自的效益函数,利用混合纳什均衡策略分析,证明在攻击方和防守方的期望效益相等时,可以达到纳什均衡。

2) 在攻防博弈中,提出部署蜜罐基站的策略,蜜罐基站不是阻止攻击者进行攻击,而是通过欺骗攻击者,诱导攻击者控制对整个网络影响相对较小的不关键基站,来减少恶意基站的数量,从而提高车联网数据传输的可靠性。

3) 利用传输时延作为反馈评价值,进一步调整蜜罐基站的欺骗策略,联合考虑数据传输时延和车联网数据传输安全性能,在保证较低传输时延情况下提高数据传输过程中的安全性。

1 相关工作

1.1 网络欺骗和攻防博弈

随着网络攻防与车联网技术的不断融合演进,安全威胁面临着巨大的挑战,如何有效降低黑客恶意攻击的影响,是一个亟待解决的问题。网络欺骗技术在安全防御研究中得到广泛关注,网络欺骗是指为攻击者提供错误的信息来迷惑攻击者,从而误导攻击者的行为^[2]。为了解决网络系统中被恶意攻击的问题,胡永进等^[3]提出一种网络欺骗博弈模型,该模型增加了网络欺骗博弈中的攻击难度,使防御者能在短时间内进行更好的防御;Jajodia 等^[4]提出了一种基于概率逻辑理论的欺骗防御(PLD, probabilistic logic deception)方案并对攻击者状态进行建模,通过为各种扫描查询提供真假混合的响应,来增加攻击者的攻击

时间和成本,以减少攻击造成的影响;石乐义等^[5]将网络诱骗攻防视作一种可观察行为的多阶段信令博弈,运用信令博弈理论分步骤构建了4种网络诱骗攻防博弈模型,并通过仿真测试验证了博弈理论贝叶斯均衡策略的存在性和正确性。上述方案利用网络欺骗技术降低了攻击者成功的可能性,提高了防守方的防御水平以及效益,为本文研究提供了思路,但采用的欺骗策略是静态策略,难以适应真实场景下动态变化的网络环境,并且忽略传输时延对于网络高效传输的影响,从而导致传输质量下降,影响用户体验质量。

在与攻防博弈相关的研究方面,攻击方和防御方有多种策略可供选择,博弈论能够解决策略相互依存环境中如何决策以获得最大收益的问题,基于攻防博弈的网络防御决策方法日益成为研究热点^[6]。针对物联网中的安全风险问题,La 等^[7]在蜜罐网络中通过攻防博弈模型将问题建模为一个不完全信息的贝叶斯博弈,在混淆攻击者的同时降低攻击者成功的概率。然而,文献[7]并未考虑传输时延对于物联网通信的影响,导致模型难以实现高效传输的目标。文献[8]针对恶意基站影响缓存安全性的问题,提出一种适用于多归属用户的异构网络安全缓存方案,并采用逆向归纳法对博弈进行分析,得到博弈双方利润最大化的 Stackelberg 均衡。该方案未结合真实攻防场景下用户的体验反馈,导致防御方案难以动态适应复杂网络下的攻防问题。Yao 等^[9]针对无线通信网络中存在多个不可信中继的安全传输问题,提出了一种基于 Stackelberg 博弈的中继选择方法,帮助源节点转发信号,从而提高系统的安全率。然而,该方案建立的模型过于单一,未考虑通过不可信中继节点进行转发所需的时延因素,导致模型的适用性降低。上述方案在分析攻防双方对抗策略时,结合了攻防博弈理论,为本文攻防博弈模型的建立与分析提供了新的思路。

1.2 车联网数据传输

为了提高车联网中数据传输的安全性,Makarfi 等^[10]提出了一个由合法接收者和窃听者组成的车辆网络的 PLS 框架,得到系统性能与窃听者车辆位置的不确定性密切相关。Sedjelmaci 等^[11]针对车联网易受不可信网络攻击的问题,提

出了一个基于层次协作博弈的网络防御框架来保护合法车辆免受攻击,通过参与者的相互合作,对可疑攻击进行检测、预测和有效反应,达到减少处理时延和开销的目标。然而,该方案考虑的指标有限,难以适应更复杂的网络场景。Liu 等^[12]提出了一种基于无人机辅助的车联网安全通信(UVSC, UAV-assisted vehicle networking security communication)方案,并利用攻防博弈理论来模拟普通无人机和干扰者之间的交互作用,利用反向归纳法对所提出的对策问题进行分析,得到博弈纳什均衡解。然而,该方案未具体考虑传输时延对于车辆请求数据的影响,并且防御方的策略复杂性不足,难以有效抵御攻击者的攻击。

当前车联网安全领域的研究,大多只是解决攻防双方策略选择与对抗的问题,很少有结合蜜罐防御策略来提升数据传输安全性能的研究,且在考虑应用场景下网络安全传输和时延限制的问题时,缺乏将时延反馈与车联网安全传输的联合分析,导致所构建的模型不够全面,难以验证在恶意攻击存在的情况下车联网数据传输质量。随着数据流量的不断增长和用户对无线服务需求的多样化,在内容高效转发与缓存方面,本文提出了 5G 车联网中以信息为中心的社会感知流媒体缓存和转发策略^[13],有效提升了网络传输性能。在安全传输方面,本文提出了一种高效可靠的多媒

体服务优化机制^[14],并利用博弈理论对问题进行求解。针对无线通信网络中的数据安全传输问题,本文基于攻防博弈理论建立了一种新颖的车联网安全传输模型,主要优势是将网络欺骗策略应用到模型中,在部署蜜罐基站后,对攻击者进行混淆欺骗,使攻击者成本提高,提升了车联网应对身份伪造攻击的能力,并分析蜜罐基站构建的可行性,通过车辆的时延反馈进一步调整蜜罐基站的欺骗策略,当车辆接收数据后返回时延反馈值给防守方时,通过调整蜜罐基站与车辆的交互性和 IP 随机化程度^[15],使防守方的整体效益得到有效提升,同时在保证数据传输过程中安全性的前提下,有效降低时延,提高车联网的服务质量。

2 系统模型

本节首先介绍攻防博弈的网络模型,接着介绍信道模型,最后介绍基于时延的反馈模型。

2.1 网络模型

系统模型由可信基站、蜜罐基站、恶意基站和车辆组成,如图 1 所示。可信基站由服务提供商部署在靠近车辆的地方,可以给车辆提供高效的计算缓存服务,如车载导航、路况信息共享等,对于智能交通具有重要意义。将同一区域中的可信基站定义为 $\mathcal{B} = \{1, 2, 3, \dots, E\}$,网络中的每个可信基站都配备了一个缓存服务器,为车联网提供

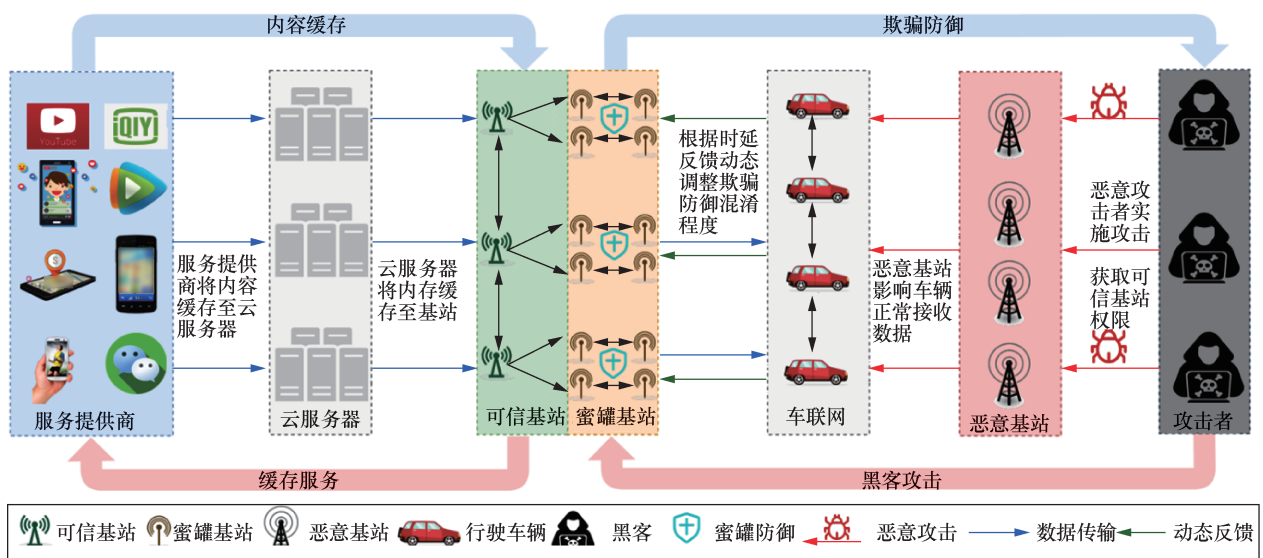


图 1 系统模型
Figure 1 System model

缓存服务。

恶意攻击者通过攻击，进而获得可信基站的控制权，将可信基站变为恶意基站，这样会干扰车辆的数据传输，如给车辆发送恶意数据导致车辆无法接收正常的的数据，或者在数据传输过程中篡改内容，导致车辆接收到错误的信息，引发交通安全事故。将攻击者控制的恶意基站定义为 $\mathcal{H} = \{1, 2, 3, \dots, H\}$ ，恶意基站通过干扰下行链路，影响数据传输质量。

车辆在行驶过程中，需要实时获取一些服务，如地图导航、车载娱乐、碰撞预警等。将车辆定义为 $\mathcal{V} = \{1, 2, 3, \dots, V\}$ ，假设每辆车都可以从多个可信基站获取缓存服务。车辆也可能收到来自恶意攻击者发送的干扰数据，从而影响服务质量，当车辆获取到数据后，根据服务质量将时延反馈给基站，当基站收到反馈判断是否受到恶意攻击者的攻击，及时调整策略，提高服务质量。

蜜罐基站部署在可信基站附近，能够欺骗混淆攻击者，将蜜罐基站定义为 $\mathcal{I} = \{1, 2, 3, \dots, I\}$ ，蜜罐基站部署的位置与可信基站接近，起到隐藏身份的作用，在车辆向可信基站请求数据时，蜜罐基站和可信基站同时响应车辆的数据请求，蜜罐基站与车辆之间进行一些黑客感兴趣的通信数据传输，如车辆用户位置信息、系统管理后台等。如果有攻击者在网络中进行窃听，获取了诱饵通信的内容，并使用这些敏感信息（如使用诱饵登录凭证）登录系统，蜜罐基站就能发现网络攻击。在这种情况下，由于网络流量繁多且难以辨识，可以达到混淆攻击者的目的，当攻击者对蜜罐基站进行攻击时，攻击者的攻击成本大大增加。

2.2 信道模型

本文所采用的通信模型为视距（LOS, line of sight）无线传输模型，将其应用于车辆与基站之间的通信^[16]。首先是防御方的相关定义，在某个时刻 t 内，将车辆 v 所在的位置定义为 (x_v, y_v) ，可信基站是固定位置，将其定义为 (x_e, y_e) ，可信基站 e 与车辆 v 距离为 $d_{e,v}(t) = \sqrt{(x_e - x_v(t))^2 + (y_e - y_v(t))^2}$ 。蜜罐基站同样是固定位置，将其位置定义为 (x_i, y_i) ，将蜜罐基站的混淆欺骗质量定义为 q_i ，混淆欺骗质量与蜜罐基站 IP 随机化以及车辆的交互性有关，混淆欺骗

质量值增大，代表蜜罐基站与车辆之间的交互性提高，防守方节点 IP 随机化程度提高，使攻击者的攻击成本增加，欺骗防御质量得到提升。

接下来是攻击方的相关定义。攻击者控制的恶意基站，假定在时刻 t 的初始位置定义为 (x_h, y_h) ，黑客通过攻击基站服务器，获取权限控制服务器，从而向车辆发送恶意数据，导致车辆无法接收正常的的数据。攻击者控制的恶意基站 h 与车辆 v 之间的距离为 $d_{h,v}(t) = \sqrt{(x_h - x_v(t))^2 + (y_h - y_v(t))^2}$ 。

将基站 e 和车辆 v 之间的信道增益定义为 $\alpha_{e,v}(t)$ ，计算如式(1)所示。

$$\alpha_{e,v}(t) = \frac{\lambda}{d_{e,v}(t)^\varepsilon} = \frac{\lambda}{(\sqrt{(x_e - x_v(t))^2 + (y_e - y_v(t))^2})^\varepsilon} \quad (1)$$

其中， λ 代表信道功率增益， ε 是路径损失指数，且 $\varepsilon > 1$ 。

同理，恶意基站 h 和车辆 v 之间的信道增益定义为 $\beta_{h,v}(t)$ ，如式(2)所示，蜜罐基站 i 与车辆 v 之间的信道增益定义为 $\gamma_{i,v}(t)$ ，如式(3)所示。

$$\beta_{h,v}(t) = \frac{\lambda a_h}{d_{h,v}(t)^\varepsilon} = \frac{\lambda a_h}{(\sqrt{(x_h - x_v(t))^2 + (y_h - y_v(t))^2})^\varepsilon} \quad (2)$$

$$\gamma_{i,v}(t) = \frac{\lambda}{d_{i,v}(t)^\varepsilon} = \frac{\lambda}{(\sqrt{(x_i - x_v(t))^2 + (y_i - y_v(t))^2})^\varepsilon} \quad (3)$$

其中 $a_h = \{0, 1\}$ ，0 表示攻击者不采取攻击，1 表示攻击者进行攻击。

可信基站 e 与车辆 v 之间的数据传输功率定义为 $p_e, e \in (1, 2, 3, \dots, E)$ ，蜜罐基站 i 与车辆 v 之间的数据传输功率定义为 $p_i, i \in (1, 2, 3, \dots, I)$ ，恶意基站 h 与车辆 v 之间的数据传输功率定义为 $p_h, h \in (1, 2, 3, \dots, H)$ 。背景噪声定义为 N ，不同基站之间会发生通信链路干扰，并且有恶意基站的干扰，将车辆在时刻 t 的信噪比定义为 $\omega_v^e(t)$ 。

$$\omega_v^e(t) = \frac{p_e \alpha_{e,v}(t)}{N + p_h \beta_{h,v}(t) + p_i \gamma_{i,v}(t) + \mu_{-}\{-e, v\}(t)} \quad (4)$$

在没有干扰时，意味着攻击者对蜜罐基站进行了攻击，未影响正常通信，此时可信基站 e 与

车辆 v 信噪比为 $\zeta_v^e(t)$ ，如式(5)所示。

$$\zeta_v^e(t) = \frac{p_e \alpha_{e,v}(t)}{N + p_i \gamma_{i,v}(t) + \mu_- \{-e, v\}(t)} \quad (5)$$

其中， $\mu_- \{-e, v\}(t)$ 是除可信基站 e 外其他可信基站所产生的信道干扰，如式(6)所示。

$$\begin{aligned} \mu_- \{-e, v\}(t) &= \sum_{\substack{e' \in E \\ e' \neq e}} p_{e'} \frac{\lambda}{d_{e',v}(t)^\epsilon} = \\ &= \sum_{\substack{e' \in E \\ e' \neq e}} p_{e'} \frac{\lambda}{(\sqrt{(x_{e'} - x_v(t))^2 + (y_{e'} - y_v(t))^2})^\epsilon} \end{aligned} \quad (6)$$

当恶意基站干扰时，根据香农定理，可信基站 e 与车辆 v 之间的数据传输率为 $C_{\omega_v^e}(B)$ ，如式(7)所示。

$$\begin{aligned} C_{\omega_v^e}(B) &= \\ &= \text{Blb} \left(1 + \frac{p_e \alpha_{e,v}(t)}{N + p_h \beta_{h,v}(t) + p_i \gamma_{i,v}(t) + \mu_- \{-e, v\}(t)} \right) \end{aligned} \quad (7)$$

同理，当恶意基站没有干扰时，可信基站 e 与车辆 v 之间的数据传输率为 $C_{\zeta_v^e}(B)$ ，如式(8)所示。

$$\begin{aligned} C_{\zeta_v^e}(B) &= \\ &= \text{Blb} \left(1 + \frac{p_e \alpha_{e,v}(t)}{N + p_i \gamma_{i,v}(t) + \mu_- \{-e, v\}(t)} \right) \end{aligned} \quad (8)$$

2.3 基于时延的反馈模型

本节考虑车联网与基站之间进行数据传输时的反馈模型，通信场景中包含 E 个可信基站、 V 个车辆、 I 个蜜罐基站、 H 个攻击者控制的恶意基站。当恶意基站干扰传输时，可信基站和蜜罐基站需要考虑如何调整传输策略来获得有效的数据传输，为了向车辆传输数据，可信基站的目标是在 t 时间周期内将尽可能多的数据传输到车辆，恶意基站会干扰下行链路，影响数据的传输质量。将车联网中可信基站发送给车辆请求的计算数据定义为 $\mathcal{M} = \{1, 2, 3, \dots, M\}$ ，将数据大小定义为 l_m 。

在受到恶意基站干扰时，从可信基站 e 到车辆 v 的数据传输时延为 $t_{\omega_v^e}$ ，如式(9)所示。

$$t_{\omega_v^e} = \frac{l_m}{C_{\omega_v^e}(B)} \quad (9)$$

同理，在没有受到恶意基站干扰时，从可信基站 e 到车辆 v 的数据传输时延为 $t_{\zeta_v^e}$ ，如式(10)所示。

$$t_{\zeta_v^e} = \frac{l_m}{C_{\zeta_v^e}(B)} \quad (10)$$

车辆根据传输时延及时反馈，当传输时延较大时，反馈评价值较小，表示服务体验质量较差，此时，对蜜罐基站的防御参数进行调整，提高混淆质量；当传输时延较小时，反馈评价值较大，表示服务体验质量较好。反馈评价值表示为 τ ，如式(11)所示。

$$\tau = \frac{\rho}{t_o} \quad (11)$$

其中， ρ 代表反馈调整参数， $\rho = t_v - t_o$ ， $t_o = \{t_{\omega_v^e}, t_{\zeta_v^e}\}$ ， t_v 表示车辆接收请求数据的约定传输时延， t_o 表示车辆接收请求数据的实际传输时延。蜜罐欺骗质量更新公式如式(12)所示^[17]。

$$\begin{aligned} \Delta q &= 1 - e^\tau \\ q_{\text{new}} &= q_i + \Delta q \end{aligned} \quad (12)$$

当实际传输时延比约定传输时延提前较多时，车联网传输受到恶意干扰的影响较小，此时反馈调整参数较大，说明反馈评价值较高，此时 $\Delta q < 0$ ，更新后的欺骗防御质量降低。反之，当反馈评价值较低时， $\Delta q > 0$ ，更新后的欺骗防御质量得到提高，车联网受到恶意攻击者干扰，此时蜜罐基站动态调整欺骗防御策略，提高交互性以及 IP 随机化程度，从而达到混淆攻击者的目的。经过多轮的迭代，攻防双方不断调整策略，达到较为稳定的平衡。

3 攻防博弈问题描述

3.1 攻防博弈模型描述

首先，将攻击者控制的恶意基站作为攻击方，将可信基站与蜜罐基站作为防守方，同时考虑蜜罐基站混淆欺骗的策略，基于进攻和防御方的效用函数找到其纳什均衡，并经过基于时延的反馈调整机制，在不断迭代过程中，找到最优的纳什均衡。

接下来，建立攻防博弈模型，先定义防守方每单位传输功率的传输成本为 c_e ，由于可信基站

与蜜罐基站同为防守方，双方传输成本定义相等。当每单位传输功率为 p_e 时，可信基站 e 的总传输成本为 $\phi_e = p_e c_e$ ，同理被攻击者所控制的恶意基站总传输成本为 $\phi_h = p_h c_h$ 。用 g_e 表示可信基站是否传输， $g_e = \{0, 1\}$ ，当 $g_e = 1$ 时，表示可信基站向车辆传输数据，否则表示不传输。同理，用 g_h 表示是否干扰攻击，当 $g_h = 1$ ，表示恶意基站对车辆进行攻击，否则表示不攻击。

然后，将攻防博弈模型定义为 $\Omega = \{E, I, H\}$ ， $\{p_e, p_i\}_{e \in E, i \in I}, \{p_h\}_{h \in H}, \{U_e\}_{e \in E}, \{U_h\}_{h \in H}$ ，本文的攻防博弈模型可视为零和博弈，攻击者和防御者双方通过相互限制得到更大的利益，可信基站的效益不仅与自身效益和成本有关，而且与恶意基站的成本有关。将可信基站的效益函数定义为 $U_{e, e \in E}$ ，如式(13)所示。

$$U_{e, e \in E} = \text{Blb}(1 + \frac{p_e \alpha_{e,v}(t) g_e}{N + p_h \beta_{h,v}(t) + p_i \gamma_{i,v}(t) + \mu_- \{-e, v\}(t)}) + (\kappa q_i - p_i c_e) g_e - p_e c_e g_e + p_h c_h g_h \quad (13)$$

其中， κ 为混淆欺骗调整参数， $q_i \in [1, 100]$ 代表混淆质量，令 $\phi_i = (\kappa q_i - p_i c_e)$ 。混淆质量定义为 $q_i = \theta a_i + (1 - \theta) b_i$ ($0 \leq \theta \leq 1$)， a_i 表示蜜罐基站与车辆的交互程度参数， b_i 表示蜜罐基站 IP 随机化参数， θ 表示交互程度影响蜜罐欺骗质量的百分比， $1 - \theta$ 表示 IP 随机化影响蜜罐欺骗质量的百分比。当数据传输时延较高时，蜜罐基站适当提升交互性和 IP 随机化程度，通过诱骗攻击者进而提高攻击者的攻击成本。

同理，恶意基站的效益函数为 $U_{h, h \in H}$ ，如式(14)所示。

$$U_{h, h \in H} = p_e c_e g_e - (\kappa q_i - p_i c_e) g_e - p_h c_h g_h - \text{Blb}(1 + \frac{p_e \alpha_{e,v}(t) g_e}{N + p_h \beta_{h,v}(t) + p_i \gamma_{i,v}(t) + \mu_- \{-e, v\}(t)}) \quad (14)$$

在攻防博弈模型中，由于双方是对立的，其中任何一方改变其策略，都会改变博弈参与双方的效益。使用零和博弈来模拟这种攻防交互的好处在于一方的收益是另一方的损失，可以更好地反映对立的程度。所以，零和博弈可以更好地反映可信基站和恶意基站之间的对抗，这样双方才

能最大化其效用。

3.2 攻防双方的效益函数矩阵

本节分析在博弈过程中可信基站和恶意基站各自的策略，由于双方都有两种策略可以选择，组合后共有 4 种，这 4 种情况的详细说明如下。

(1) 当可信基站传输恶意基站攻击时，可信基站的效益函数为

$$U_{e, e \in E} = C_{\omega_e^c}(B) - \phi_e + \phi_h + \phi_i \quad (15)$$

此时恶意基站的效益函数为

$$U_{h, h \in H} = \phi_e - C_{\omega_h^c}(B) - \phi_h - \phi_i \quad (16)$$

(2) 当可信基站不传输、恶意基站攻击时，可信基站的效益函数为

$$U_{e, e \in E} = \phi_h \quad (17)$$

此时恶意基站的效益函数为

$$U_{h, h \in H} = -\phi_h \quad (18)$$

(3) 当可信基站传输数据、恶意基站不干扰时，可信基站的效益函数为

$$U_{e, e \in E} = C_{\zeta_v^e}(B) - \phi_e + \phi_i \quad (19)$$

此时恶意基站的效益函数为

$$U_{h, h \in H} = \phi_e - C_{\zeta_v^e}(B) - \phi_i \quad (20)$$

(4) 当可信基站不传输、恶意基站不干扰时，双方的效益都为 0。

假设在这个情况下，可信基站和蜜罐基站的传输效益比维护安全所需费用高，可信基站有理由向车辆传输数据。攻防双方在不同策略下效用函数矩阵如图 2 所示。

	可信基站传输	可信基站不传输
恶意基站攻击	$\phi_e - C_{\omega_e^c}(B) - \phi_h - \phi_i,$ $C_{\omega_e^c}(B) - \phi_e + \phi_h + \phi_i$	$-\phi_h, \phi_h$
恶意基站不攻击	$\phi_e - C_{\zeta_v^e}(B) - \phi_i,$ $C_{\zeta_v^e}(B) - \phi_e + \phi_i$	0, 0

图 2 攻防效益函数矩阵

Figure 2 Attack and defense benefit function matrix

3.3 混合策略纳什均衡分析

将攻防博弈视为一个零和博弈，攻防双方有着各自的策略，组合成 4 种情况。本文假设博弈

中的参与人是理性的,理性的参与者要考虑代价。在相同收益情况下,参与者需要考虑更低成本的攻击和防御方式。因此,在博弈的过程中,双方需要选择合适的策略使自己的收益最优。

在这个博弈过程中,没有纯策略纳什均衡,因为双方都有各自的最优策略,故需要利用混合策略纳什均衡分析来解决问题。

定义 1 对于攻防博弈,混合纳什均衡是任何参与者在纯策略集 S 上的概率分布 p , 即 $p = (p_1, p_2, p_3, \dots, p_r) \in \mathbb{R} \geq 0$, 其中 $\sum_{i=1}^R p_i = 1$ 。

对于可信基站,定义其传输数据的概率为 P_T , 不传输数据的概率为 P_{NT} ; 定义恶意基站干扰的概率为 P_A , 不干扰的概率为 P_{NA} , 如图 3 所示。

	P_T	P_{NT}
P_A	$\phi_e - C_{\omega_v^e}(B) - \phi_h - \phi_i,$ $C_{\omega_v^e}(B) - \phi_e + \phi_h + \phi_i$	$-\phi_h, \phi_h$
P_{NA}	$\phi_e - C_{\zeta_v^e}(B) - \phi_i$ $C_{\zeta_v^e}(B) - \phi_e + \phi_i$	0, 0

图 3 攻防策略效益函数矩阵
Figure 3 Attack and defense strategy benefit function matrix

根据混合纳什均衡的定义,当可信基站与恶意基站的期望效益相等时,参与者将不再关心策略的选择。因此,在所提的博弈模型中,混合策略使攻击方在干扰与不干扰时的期望效益相同,防御方在传输和不传输时的期望效益相同。

令 $E(P_T) = E(P_{NT})$, $E(P_A) = E(P_{NA})$ 得到攻防双方的混合策略,具体分析如下。

$$\begin{cases} E(P_T) = E(P_{NT}) \\ E(P_T) = P_A \cdot (C_{\omega_v^e}(B) - \phi_e + \phi_h + \phi_i) + \\ P_{NA} \cdot (C_{\zeta_v^e}(B) - \phi_e + \phi_i) \\ E(P_{NT}) = P_A \cdot \phi_h + P_{NA} \cdot 0 \end{cases} \quad (21)$$

$$\begin{cases} E(P_A) = E(P_{NA}) \\ E(P_A) = P_T \cdot (\phi_e - C_{\omega_v^e}(B) - \phi_h - \phi_i) + P_{NT} \cdot (-\phi_h) \\ E(P_{NA}) = P_T \cdot (\phi_e - C_{\zeta_v^e}(B) - \phi_i) + P_{NT} \cdot 0 \end{cases} \quad (22)$$

由式(21)、式(22)得攻防双方的混合纳什均衡如下。

$$P_T = \frac{\phi_h}{C_{\zeta_v^e}(B) - C_{\omega_v^e}(B)}, P_{NT} = 1 - \frac{\phi_h}{C_{\zeta_v^e}(B) - C_{\omega_v^e}(B)} \quad (23)$$

$$P_A = \frac{\phi_e - C_{\zeta_v^e}(B) - \phi_i}{C_{\omega_v^e}(B) - C_{\zeta_v^e}(B)}, P_{NA} = 1 - \frac{\phi_e - C_{\zeta_v^e}(B) - \phi_i}{C_{\omega_v^e}(B) - C_{\zeta_v^e}(B)} \quad (24)$$

通过计算得到各自策略的概率,在攻防博弈过程中,最终得到混合纳什均衡,即所得概率集。在这个概率集中,双方的效用可以同时达到最优情况,假定双方遵守规则约定,任何一方都不会改变策略来打破平衡,即达到混合纳什均衡。

4 实验模拟

本节主要介绍实验模拟环境以及结果分析,实验利用 Python3.7 进行模拟,测试运行环境为 Intel Core i7-7700HQ CPU @ 2.80 GHz 的处理器,运行内存为 8 GB,操作系统是 Windows10 64 位操作系统。仿真场景由可信基站、蜜罐基站、恶意基站和车辆组成,其中可信基站为车辆提供数据传输服务,蜜罐基站诱导恶意攻击者进行攻击,从而提高可信基站的传输可靠性,恶意基站是通过干扰数据传输来提升自身的效益。

在仿真实验中,可信基站个数设置为 10 个,车辆数量设置为 50 个,恶意基站设为 1 个,蜜罐基站设为 5 个,区域大小设置为 1000 m×1 000 m。本文采用基于时延反馈的蜜罐防御策略(BTHD),对比方案是基于文献[4]的无时延反馈方案(PLD)和文献[15]的无蜜罐防御方案(UVSC)。实验分析指标为可信基站的效益、传输概率和干扰概率(混合纳什均衡)、数据传输率、数据传输时延、时延反馈评价值和防守方期望效益,通过分析对比不同方案情况下的指标变化,验证了所提策略在有干扰攻击的情况下车联网数据传输时的性能优势。

图 4 表示有无恶意攻击情况下可信基站效益。由图可知,在迭代初期,变化幅度较为平缓,随后攻防双方不断交互博弈,在有恶意干扰情况下可信基站效益趋于无恶意干扰时的效益,说明蜜罐防御策略能在一定程度上抵御恶意攻击,提升防守方的效益,并且整体上在无恶意攻击的情

况下,可信基站的效益高于存在恶意攻击的情况。同时 BTHD 策略可信基站的效益在整体上高于对比的 UVSC 方案。

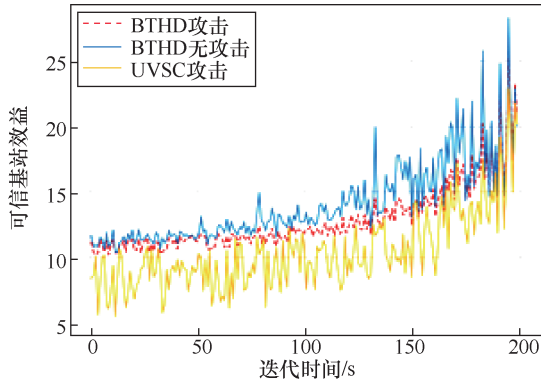


图4 有无恶意攻击情况下可信基站效益
Figure 4 Benefits of trusted base stations with or without malicious attacks

图5表示不同蜜罐混淆程度下的传输概率和干扰概率。蜜罐混淆程度与蜜罐欺骗质量相同,由蜜罐基站与车辆的交互性和IP随机化程度共同决定。从图5中可以分析,当蜜罐混淆程度提高时,恶意基站干扰的概率降低,由于蜜罐欺骗防御质量的提升,结合蜜罐欺骗质量公式,此时蜜罐基站与车辆的交互性与IP随机化程度提高,恶意攻击者的攻击成本大大增加。可信基站传输数据的概率随着蜜罐欺骗混淆程度的增大而提高,说明蜜罐基站对于可信基站与车辆之间的数据通信进行了保护,使攻击者难以有效实施攻击。

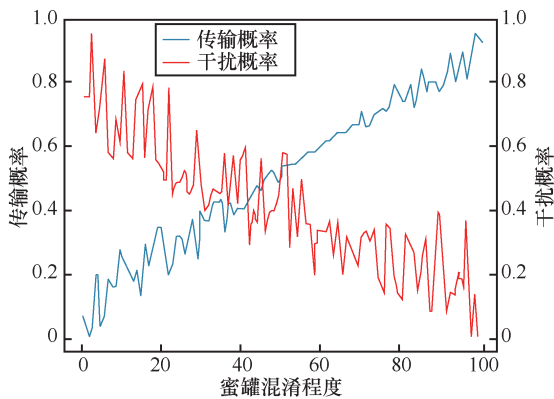


图5 不同蜜罐混淆程度下的传输概率和干扰概率
Figure 5 Transmission probability and interference probability under different levels of honeypot confusion

从图6中可以分析数据传输率随迭代时间的变化,BTHD策略在无恶意攻击时的数据传输率

比存在恶意攻击时高,说明在恶意攻击者对通信过程进行干扰破坏时,导致车辆无法正常接收数据,使数据传输率下降。同时,BTHD策略在有无恶意干扰攻击的情况下数据传输率都比无蜜罐防御方案UVSC高,说明蜜罐防御对于提升网络传输性能具有重要意义。随着时间的不断迭代,调整蜜罐的混淆策略,可以减少干扰的影响,但同时蜜罐策略调整后对于正常的数据传输存在影响,在经过一段时间的迭代后,无干扰时数据传输率与干扰存在时的情况基本相等,达到最终的平衡。

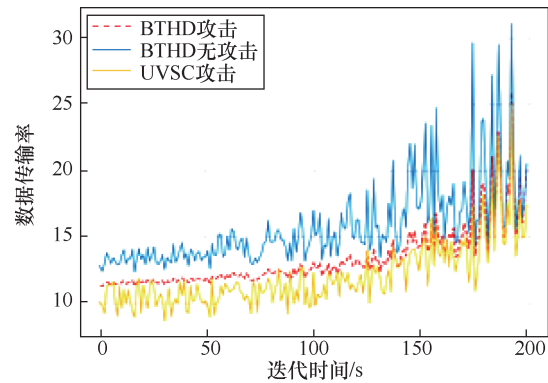


图6 数据传输率随迭代时间的变化
Figure 6 Data transfer rate varies with iteration time

图7表示数据传输时延随迭代时间变化,从图中可以分析,在恶意攻击存在时数据传输时延比无恶意攻击时高,时延过大时说明干扰过多,当采用基于时延的反馈调整策略时,经过一段时间迭代,存在恶意干扰时的数据传输时延不断逼近无恶意攻击时的情况,并且从整体分析,数据传输时延呈下降趋势,说明蜜罐防御策略对于攻击者的攻击具有抵御作用。同时从整体分析对比方案UVSC,无蜜罐防御导致攻击者成功控制可信基站的概率增大,其传输时延高于本文策略。

时延反馈评价随迭代时间变化如图8所示。时延反馈评价可以反映车辆对于可信基站提供服务的质量评价,时延反馈评价越高,数据传输时延越小,通信质量越高。通过对比分析,本文策略在有无攻击的情况下时延反馈评价比UVSC方案高,同时随着时间的不断迭代,时延反馈评价在有无恶意攻击和无恶意攻击的情况下

趋于相等,说明蜜罐欺骗防御策略能改善车辆的服务体验质量。

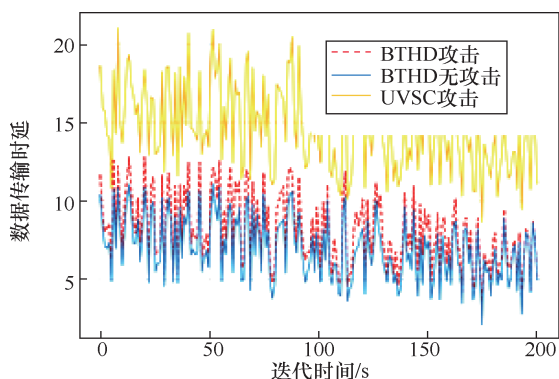


图7 数据传输时延随迭代时间变化

Figure 7 Data transmission delay varies with iteration time

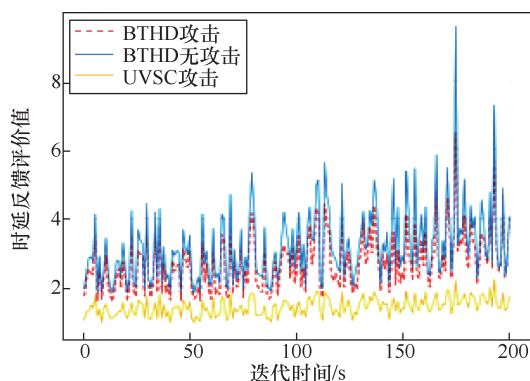


图8 时延反馈评价随迭代时间变化

Figure 8 Delay feedback evaluation changes with iteration time

不同方案下防守方期望效益随蜜罐混淆程度变化如图9所示,从图9中可以分析,本文所提基于零和博弈的蜜罐欺骗防御策略能有效提升防守方的期望效益,对于另外两种方案具有明显的优势。UVSC方案是攻防双方采用无蜜罐防御情况下的混合纳什均衡策略选择各自的行动,导致期望收益较低。PLD方案是采用蜜罐防御策略但缺乏时延反馈动态调整攻防双方策略,当蜜罐混淆程度较高时,蜜罐部署影响了正常的数据通信,导致期望收益降低。在混淆程度较低时,本文策略与PLD方案所得期望效益相差不大,随着蜜罐混淆程度的提升,本文策略与PLD方案的期望收益差值逐渐增大,本文策略的优势逐渐体现。

5 结束语

本文提出了一种结合可信基站与蜜罐基站防御攻击者干扰的策略,首先建立攻防博弈模型,

可信基站的策略为是否选择传输数据,恶意基站的策略为是否选择干扰数据传输,并将其视为一个零和博弈模型;接着分析攻防双方的效益函数,并考虑车辆接收数据的传输时延作为反馈,进一步调整攻防双方的策略,达到最后的混合纳什均衡。仿真结果表明,该策略可以在恶意攻击者存在的情况下,保证较低的传输时延,同时可以提高数据传输的可靠性。本文主要考虑了时延反馈动态调整下攻防双方策略选择的影响因素,未来工作将进一步考虑多种因素联合的动态调整反馈策略。

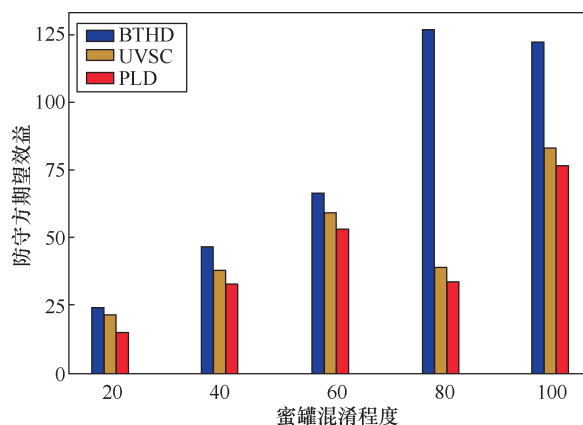


图9 不同方案下防守方期望效益随蜜罐混淆程度变化

Figure 9 The expected benefits of the defender under different schemes vary with the degree of honeypot confusion

参考文献:

- [1] 任沁沁. 全国机动车保有量达3.95亿辆,驾驶人达4.81亿人[N]. 新华每日电讯, 2022-01-12(2).
REN Q Q. There are 395 million motor vehicles in China and 481 million drivers [N]. Xinhua Daily Telegraph, 2022-01-12(2).
- [2] 杨德全, 刘卫民, 俞宙. 基于蜜罐的主动防御应用研究[J]. 网络与信息安全学报, 2018, 4(1): 57-62.
YANG D Q, LIU W M, YU Z. Research on active defense application based on honeypot[J]. Chinese Journal of Network and Information Security, 2018, 4(1): 57-62.
- [3] 胡永进, 马骏, 郭渊博. 基于博弈论的网络欺骗研究[J]. 通信学报, 2018, 39(S2): 9-18.
HU Y J, MA J, GUO Y B. Research on cyber deception based on game theory[J]. Journal of Communication, 2018, 39(S2): 9-18.
- [4] JAJODIA S. A probabilistic logic of cyber deception[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(11): 2532-2544.
- [5] 石乐义, 赵俊楠, 李芹, 等. 基于信令博弈的网络诱骗防御策略分析与仿真[J]. 系统仿真学报, 2016, 28(2): 348-353.
SHI L Y, ZHAO J N, LI Q, et al. Signaling game analysis and simulation on network decoy defense strategies[J]. Journal of System

- Simulation, 2016, 28(2): 348-353.
- [6] 刘小虎, 张恒巍, 马军强, 等. 基于攻防博弈的网络防御决策方法研究综述[J]. 网络与信息安全学报, 2022, 8(1): 1-14.
LIU X H, ZHANG H W, MA J Q, et al. Research review of network defense decision-making methods based on attack and defense game[J]. Chinese Journal of Network and Information Security, 2022, 8(1): 1-14.
- [7] 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): 1025-1035.
- [8] XU Q, SU Z, ZHANG K, Game theoretical secure caching scheme in multi-homing heterogeneous networks[C]//2018 IEEE International Conference on Communications (ICC). 2018: 1-6.
- [9] YAO R, ZHANG G, FAN Y, RABIE KM, KAIWARTYA O, et al. Untrusted relay selection and secure transmission optimization based on stack-elberg game[C]//2021 6th International Conference on Intelligent Computing and Signal Processing (ICSP). 2021: 534-539.
- [10] MAKARFIET A U, RABIE KM, KAIWARTYA O, et al. Toward physical-layer security for internet of vehicles: interference-aware modeling[J]. IEEE Internet of Things Journal, 2021, 8(1): 443-457.
- [11] SEDJELMACI H, BRAHMI I H, ANSARI N, et al. M. Cyber security framework for vehicular network based on a Hierarchical Game[J]. IEEE Transactions on Emerging Topics in Computing, 2021, 9(1): 429-440.
- [12] LIU B, SU Z, XU Q. Game theoretical secure wireless communication for UAV-assisted vehicular Internet of Things[J]. China Communications, 2021, 18(7): 147-157.
- [13] 曹腾飞, 江翠丽, 刘志强, 等. 基于信息中心 5G 车联网中社会感知的流媒体缓存与转发策略[J]. 电信科学, 2019, 35(12): 90-98.
CAO T F, JIANG C L, LIU Z Q, et al. Social-aware caching and forwarding for video streaming in information-centric 5G VANET[J]. Telecommunications Science, 2019, 35(12): 90-98.
- [14] CAO T, XUET C, Reliable and efficient multimedia service optimization for edge computing-based 5g networks: game theoretic approaches[J]. IEEE Transactions on Network and Service Management, 2020, 17(3): 1610-1625.
- [15] SUN J, SUN K. DESIR: decoy-enhanced seamless IP randomization[C]//IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications. 2016.
- [16] XIE L, SU Z, CHEN N, et al. A game theory based scheme for secure and cooperative UAV communication[C]//ICC 2021- IEEE International Conference on Communications. 2021: 1-6.
- [17] XU Q, SU Z, YU S, et al. Trust based incentive scheme to allocate big data tasks with mobile social cloud[J]. IEEE Transactions on Big Data, 2022, 8(1): 113-124.

[作者简介]



易杰 (1998-), 男, 湖北荆州人, 青海大学硕士生, 主要研究方向为网络欺骗和攻防博弈。



曹腾飞 (1987-), 男, 湖北钟祥人, 青海大学副教授、博士生导师, 主要研究方向为智能网络优化和网络攻防。



郜帅 (1980-), 男, 河南济源人, 北京交通大学教授、博士生导师, 主要研究方向为网络空间安全 and 信息网络理论及关键技术。



黄建强 (1985-), 男, 陕西西安人, 青海大学教授, 主要研究方向为移动计算、云计算和大数据。