基于博弈论的车联网延时攻击防护技术研究

于龙海　于明明　霍全瑞　孙冬青　任世轩

（中汽智联技术有限公司，天津 300393）

【摘要】针对车路协同场景下车联网（V2X）通信过程中通信信道受到干扰造成通信延时的问题，提出了基于博弈论的V2X延时攻击防护方法。以信噪比为衡量指标，基于博弈论，首先研究攻击节点传输功率与信噪比的函数关系，得到合法节点传输功率与攻击节点传输功率之间的函数关系，将其带入合法节点传输功率与信噪比的关系中，同时考虑信号传输概率、被检概率、漏检概率和其他节点的传输干扰，获得目标函数。最后，通过仿真与试验对提出的防护方法进行安全性验证，结果表明，通过调整节点传输功率，可以有效抵御攻击者对V2X通信的干扰，缩短通信延时。

主题词：车联网通信　延时攻击　信噪比　博弈论　防护技术

中图分类号：TP399　　**文献标识码：**A　　**DOI:** 10.19620/j.cnki.1000-3703.20220998

Research on V2X Delay Attack Protection Technology Based on Game Theory

Yu Longhai, Yu Mingming, Huo Quanrui, Sun Dongqing, Ren Shixuan

（CATARC Intelligent and Connected Technology Co., Ltd., Tianjin 300393）

【Abstract】For the problem of communication delay caused by the interference of the communication channel in the process of vehicle-road cooperative V2X communication, this paper proposed a V2X delay attack protection technology based on game theory. With the signal-to-noise ratio as the measurement index of communication quality, this paper firstly studied the function relationship between the transmission power of the attacking node and the signal-to-noise ratio to obtain the function relationship between the transmission power of the legitimate node and the attacking node, then this functional relationship was brought into the relationship between transmission power of legitimate node and the signal-to-noise ratio. This function also considered the probability of signal transmission, the probability of being detected and the transmission interference of other nodes to obtain the target function. Finally, the proposed protection technology is verified by simulation and test. The results show that by adjusting the transmission power of the nodes, it can effectively resist the attacker's interference on the V2X communication channel and reduce the communication delay.

Key words: V2X communication, Delay attack, Signal-to-noise ratio, Game theory, Protection technology

【引用格式】于龙海, 于明明, 霍全瑞, 等. 基于博弈论的车联网延时攻击防护技术研究[J]. 汽车技术, 2023(11): 49-55.

YU L H, YU M M, HUO Q R, et al. Research on V2X Delay Attack Protection Technology Based on Game Theory[J]. Automobile Technology, 2023(11): 49-55.

1　前言

车联网（Vehicle to everything，V2X）[1-2]能够实现人车路的有效协同，也给车辆的安全性带来了隐患。车载单元（On Board Unit，OBU）和路侧单元（Road Side Unit，RSU）在信息交互过程中容易受到信号干扰，使通信延时急剧增加，破坏信息交互连续性，进而导致人身危险及财产损失[3-4]。

文献[5]调查了针对自动驾驶汽车的各种网络攻击的可能性、严重性和可预防性，并提供了相关漏洞和防护手段。文献[6]提出了可反映道路状况的路况知识矩阵，并将该矩阵与车辆互联领域中的车辆状态进行映射，提出了车辆互联领域的安全问题与挑战。文献[7]指出了智能网联汽车领域女巫攻击的危害，车辆将多个虚假消息传输到其他节点上，通过提高恶意信息在传输窗口中的信息占比与位置随机性，模糊化攻击者的真实身份。智能网联汽车领域依旧使用密码学和公钥基础设施（Public Key Infrastructure，PKI）来保障安全性。文

献[8]提出了大规模车联网条件下的密码方案，以此加强认证，将公钥密码学引入假名生成，以非对称密码学方式获取车辆真实身份。因车联网终端通信多为无线方式，无线物理层的安全研究将极大提高车联网的鲁棒性。文献[9]、文献[10]的防护方案向通信信号中加入噪声，使得带有人为噪声的信号在空间中传播，以此提高信号传输的安全性。文献[11]研究了大规模网络场景下通信节点相互影响模型和单一节点传输模型。文献[12]研究了无线信号传输过程中的通信延时攻击，通过干扰合法传输增加延时，并基于随机几何方法建立了干扰模型。文献[13]提出了无线通信场景下基于检测被攻击频率的无线信道的防御方法。文献[14]提出了一种缓和无线通信干扰的模型，通过提高信号发射功率提升了合法传输信号的信噪比，进而防御信号干扰。

现有安全研究多集中于车辆匿名化与隐私保护、车联网PKI体系设计与建设、机器学习在车联网入侵节点检测中的应用，但对于物理层信道的攻击研究较少。本文在前期研究工作的基础上，提出一种基于博弈论的V2X延时攻击防护方法，通过调节车联网节点传输策略保证通信质量，抵御攻击者对信道的干扰，针对LTE-V2X PC5无线通信过程中的信道干扰进行防御，缩短通信延时，保证V2X应用场景的安全性、通信可靠性。

2　延时攻击防护方案

攻击者通过向V2X信道发射噪声，降低合法车联网节点的信噪比，进而增加车联网节点传输延时。根据香农定理，无线通信场景下，信号的传输功率越大，信息传递的速率也越大：

$$C=B\log_2(1+S/N) \tag{1}$$

式中，C为无线信号传输速率；B为无线信道带宽；S为信息的传输功率；N为应用环境中噪声功率。

本文研究的攻击场景中，攻击节点进行反应式干扰攻击，即攻击节点持续检测无线信道中的能量强度，所检测的信道中能量高于一定阈值即视为存在车联网节点通信，当检测到信号传输发生时，攻击节点向信道广播噪声。车联网具有极强的动态拓扑特性，因此攻击节点可能会跟随传输信号源，也可能在固定位置对周围环境进行干扰攻击。反应式干扰攻击仅在判断出信道上存在通信时发射干扰信号，因此降低了攻击的能量消耗，以此延长攻击节点生命周期，提高破坏能力。攻击流程如图1所示。

目前，国内车联网通信主要借助OBU与RSU开展。某一时刻，选取一台合法车辆作为研究对象，车辆与RSU的通信场景如图2所示。其中，P_s为OBU的信号传输功率，P_j为攻击节点噪声发射功率，h_s为OBU到RSU的信道增益，h_l为OBU到攻击节点间的信道增益，h_j为攻击节点到RSU间的信道增益。OBU与RSU通过PC5接口进行车联网通信，此时RSU可能与多台车辆进行通信。环境中存在某一攻击节点，对合法车辆进行反应式干扰攻击，以达到干扰PC5信道通信、延长车联网业务通信延时的目的。攻击节点持续检测PC5信道上的信号功率，当检测结果大于设定阈值时，判断PC5信道上存在合法OBU与RSU通信。

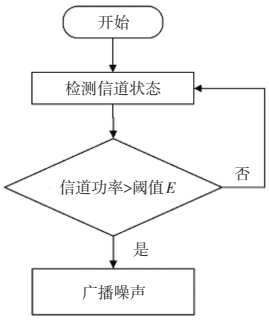

图1　恶意节点攻击流程

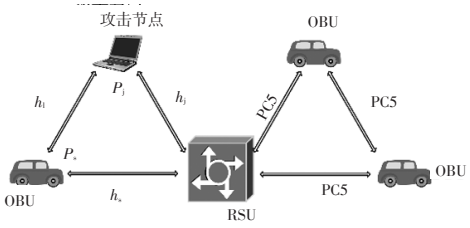

图2　攻击场景

车联网具有高度动态的拓扑特性，攻击节点会因与合法车辆的距离变化，导致检测失误。故本文借助概率来描述应用场景下的通信问题。假设合法OBU与RSU发生通信的概率为P_T，攻击节点检测到应用场景下PC5信道内合法通信的概率为P_D，设攻击节点错误检测合法通信的概率为P_F，则有：

$$\begin{cases} P_D(P_s)=G(t)\left(\left(\dfrac{E}{g}-X-1\right)\sqrt{tf_s}\right) \\ X=\dfrac{P_s h_l}{g} \\ G(t)=\dfrac{1}{\sqrt{2\pi}}\displaystyle\int_t^{\infty}\exp\left(-\frac{t^2}{2}\right)\mathrm{d}t \end{cases} \tag{2}$$

$$P_F=G(t)\left(\left(\frac{E}{g}-1\right)\sqrt{tf_s}\right) \tag{3}$$

式中，g为应用场景下环境噪声功率；X为应用场景下OBU的信噪比；E为攻击节点判断PC5信道中存在合法通信的能量功率阈值；t为攻击节点持续检测信道的检测时间；f_s为攻击节点的采样频率；$G(t)$为二维高斯分布函数，用于建立攻击节点检测概率。

攻击场景下，合法OBU传输的信噪比X为：

$$X=\frac{P_s h_s}{P_j h_j+g} \tag{4}$$

OBU传输信息的速率与信号发射功率间的关系为[15-16]：

$$\begin{cases} f(P_s)=\dfrac{P_s h_s}{P_j h_j+g}-\dfrac{2\cdot h_s}{P_j h_j P_{\max}}P_s-Y \\ Y=\displaystyle\sum_{i=1}^{k}\dfrac{\dfrac{E(s_i^2)}{\sigma^2}-1}{1-\dfrac{E(s_i^2)}{\sigma^2}+\dfrac{E(s_i^2)}{\sigma^2}\left[E(r_i)^2\right]} \end{cases} \tag{5}$$

式中，$P_{\max}$为天线的最大传输功率；Y为应用场景中其他OBU与RSU通信对所研究的OBU产生的噪声的多径效应及莱斯衰落后在环境中产生的信噪比[12]；k为环境中噪声信号的数量，除OBU自身与其他车联网单元的通信信号外，其他信号均视为对本OBU通信的噪声信号；s_i为环境中第i个噪声信号；$E(s_i^2)$为噪声信号s_i的计算功率平均值；σ^2为静态高斯分布方差；r_i为第i个信号的衰落因子；$E(r_i)$为所有信号的衰落因子的平均值。

OBU传输目标函数中包含了攻击节点的噪声功率、环境中多节点传输多径效应及莱斯衰落影响等因素的关系。目标函数通过提高信号传输过程中的信噪比来提高信息传输速率，进而缩短通信传输延时。应用环境中，同一个RSU某一时刻可能与多个OBU进行通信。这样，当研究某辆车时，其他OBU将会对研究目标的通信造成信号干扰，该干扰量即为Y。合法传输信噪比是正向激励，信号在传输过程中的能量损耗及环境噪声为负向激励。在Y模型建立过程中，由于通信场景中其他单元的通信对于所研究的OBU通信而言均为外界干扰，其他通信OBU的信号直流分量对研究对象存在严重干扰，因此选用噪声莱斯衰落后的信噪比作为负向激励。

分析攻击节点在所设计的应用场景下的信号传输。和构建车辆数据传输能力与传输功率关系的过程类似，攻击节点的目标函数为：

$$f(P_j)=-\frac{P_s h_s}{P_j h_j+g}-\frac{2\cdot h_j}{h_1 h_s P_{\max}}P_j+Y \tag{6}$$

在工作过程中，环境中OBU与RSU通信产生的Y对于攻击节点加强了攻击效果，为正向增益。式(6)中并未加入因攻击节点检测误报、漏报以及OBU通信概率的修正。当OBU正常通信，但攻击节点错误检测时，攻击节点并未发动攻击，OBU与攻击节点的目标函数为：

$$\begin{cases} f(P_s)_{P_j=0}=\dfrac{P_s h_s}{g}-\dfrac{2h_s}{h_1 h_j P_{\max}}-Y \\ f(P_j)_{P_j=0}=-\dfrac{P_s h_s}{g}+Y \end{cases} \tag{7}$$

当OBU未通信，攻击节点错误检测时，OBU与攻击节点的目标函数为：

$$\begin{cases} f(P_s)_{P_s=0}=0 \\ f(P_j)_{P_s=0}=-\dfrac{2h_j}{h_1 h_s P_{\max}}+Y \end{cases} \tag{8}$$

当应用环境中不存在PC5通信，攻击节点未攻击时，OBU与攻击节点的目标函数为：

$$\begin{cases} f(P_s)_{P_s=0,P_j=0}=0 \\ f(P_j)_{P_s=0,P_j=0}=0 \end{cases} \tag{9}$$

此时，Y不会对OBU及攻击节点的目标函数产生影响。

式(7)~式(9)分别建立了OBU与攻击节点在OBU正常通信且攻击节点错误检测时的目标函数、OBU未通信且攻击节点错误检测时的目标函数，以及OBU未通信且攻击节点正常检测时的目标函数。为了使目标函数包含所有情况，将式(2)传输检测概率、式(3)检测误报概率与车辆的信号传输概率P_T代入研究对象OBU目标函数式(5)、攻击节点目标函数式(6)中，分别得到正常通信车联网节点综合目标函数和攻击节点综合目标函数：

$$\begin{aligned} f(P_s)=&P_T\cdot P_D(P_s)\cdot\left(\frac{P_s h_s}{P_j h_j+g}-\frac{2h_s}{h_1 h_j P_{\max}}P_s-Y\right)+\\ &P_T(1-P_D(P_s))\cdot\left(\frac{P_s h_s}{g}-\frac{2h_s}{h_1 h_j P_{\max}}P_s-Y\right) \end{aligned} \tag{10}$$

$$\begin{aligned} f(P_j)=&P_T P_D(P_s)\left(-\frac{P_s h_s}{P_j h_j+g}-\frac{2h_j}{h_1 h_s P_{\max}}P_j+Y\right)+\\ &P_T(1-P_D(P_s))\cdot\left(-\frac{P_s h_s}{g}+Y\right)+\\ &(1-P_T)\cdot P_F\left(-\frac{2h_j}{h_1 h_j P_{\max}}P_j+Y\right) \end{aligned} \tag{11}$$

式(10)、式(11)表达了OBU传输效果、攻击节点攻击效果与OBU传输功率P_s、攻击节点传输功率P_j之间的关系。对于噪声Y的处理，采用三阶拟合系数，得到Y的近似解，并归一化计算偏差。莱斯衰落因子为：

$$r_i=\sqrt{(x_i+\beta)^2+y_i} \tag{12}$$

式中，x_i、y_i为不同信道内的2束静态高斯分布信号；β为该信道噪声的直视分量。

当取r_i=10 dB时，Y的近似值为10 dB。根据文献[15]的研究结论，r_i<25 dB时，Y均近似与r_i相同。即在该攻击场景下，虽然莱斯因子和车辆传输功率与环境噪声功率相关，但环境中的莱斯衰减系数在某一范围内波动，后续仿真中，可利用该结论简化仿真公式。

为了抵抗攻击，车联网节点通信时，应该考虑到攻

击节点可能的攻击情况，进而调整传输策略。针对传输目标，通信的车辆信噪比取有限范围内的最大值：

$$\begin{cases} X_{\mathrm{OBU}} = \max_{0\leqslant P_{\mathrm{s}}\leqslant P_{\max}} f(P_{\mathrm{s}}) \\ X_{\mathrm{attack}} = \max_{0\leqslant P_{\mathrm{j}}\leqslant P_{\max}} f(P_{\mathrm{j}}) \end{cases} \tag{13}$$

式中，X_{OBU}为攻击场景下OBU的信噪比最大值；X_{attack}为攻击场景下攻击节点的信噪比最大值。

OBU与攻击节点两者的信噪比在应用场景中是相互影响的。在攻击模型中，OBU与攻击节点在时间维度上存在联系。OBU与RSU开始通信，随后攻击节点检测PC5信道上的能量，检测到V2X通信后发动攻击。OBU根据传输信噪比调整传输策略。本文基于博弈论方法分析目标函数，首先分析攻击节点，在攻击节点传输策略固定的条件下分析OBU的通信情况，通过一次博弈，得到OBU的传输策略。计算攻击节点目标函数$f(P_{\mathrm{j}})$取得极大值时的攻击功率P_{j}及$f(P_{\mathrm{j}})$关于P_{j}一阶导数为0的点，将该点带入攻击节点综合目标函数式(11)中，得到P_{s}与P_{j}的关系：

$$P_{\mathrm{j}} = \begin{cases} \dfrac{1}{h_{\mathrm{j}}}\left[\dfrac{P_{\mathrm{T}}P_{\mathrm{D}}(P_{\mathrm{s}})h_{\mathrm{s}}h_{\mathrm{j}}P_{\max}}{2h_{\mathrm{j}}\left[P_{\mathrm{T}}P_{\mathrm{D}}(P_{\mathrm{s}})+(1-P_{\mathrm{T}})P_{\mathrm{F}}\right]}\right], \\ \dfrac{P_{\mathrm{T}}P_{\mathrm{D}}(P_{\mathrm{s}})}{P_{\mathrm{T}}P_{\mathrm{D}}(P_{\mathrm{s}})+(1-P_{\mathrm{T}})P_{\mathrm{F}}} \geqslant \dfrac{2gh_{\mathrm{j}}}{h_{\mathrm{s}}^2h_1P_{\max}} \\ 0,\text{其他} \end{cases} \tag{14}$$

从攻击节点分析传输策略，在车辆传输策略固定，即P_{s}固定的条件下计算P_{j}，然后导出P_{j}关于P_{s}的函数关系，得出此时能够检测到的P_{s}的值与检测率$P_{\mathrm{D}}(P_{\mathrm{s}})$间的关系。攻击节点可检测功率$f_{\mathrm{T}}(P_{\mathrm{s}})$与$P_{\mathrm{s}}$的函数为：

$$f_{\mathrm{T}}(P_{\mathrm{s}}) = \frac{P_{\mathrm{T}}P_{\mathrm{D}}(P_{\mathrm{s}})P_{\mathrm{s}}}{P_{\mathrm{T}}P_{\mathrm{D}}(P_{\mathrm{s}})+(1-P_{\mathrm{T}})P_{\mathrm{F}}} \tag{15}$$

分析$f_{\mathrm{T}}(P_{\mathrm{s}})$的变化规律，先计算$f_{\mathrm{T}}(P_{\mathrm{s}})$关于$P_{\mathrm{s}}$的一阶偏导数：

$$\frac{\partial f_{\mathrm{T}}}{\partial P_{\mathrm{s}}} = \frac{P_{\mathrm{T}}(1-P_{\mathrm{T}})P_{\mathrm{D}}'(P_{\mathrm{s}})P_{\mathrm{F}}}{\left[P_{\mathrm{T}}P_{\mathrm{D}}(P_{\mathrm{s}})+(1-P_{\mathrm{T}})P_{\mathrm{F}}\right]^2} + \frac{P_{\mathrm{T}}P_{\mathrm{D}}(P_{\mathrm{s}})}{P_{\mathrm{T}}P_{\mathrm{D}}(P_{\mathrm{s}})+(1-P_{\mathrm{T}})P_{\mathrm{F}}} \tag{16}$$

其中，$P_{\mathrm{D}}(P_{\mathrm{s}})$的导数$P_{\mathrm{D}}'(P_{\mathrm{s}})$可由式(2)计算，结果为：

$$P_{\mathrm{D}}'(P_{\mathrm{s}}) = \frac{1}{\sqrt{2\pi}}\exp\left(-\frac{\left(\dfrac{E}{g}-X-1\right)^2}{2(2X+1)}\right)\cdot\frac{1}{\sqrt{2X+1}}\cdot \frac{\dfrac{E}{g}+X}{2X+1}\cdot\frac{h_1}{g} \tag{17}$$

$P_{\mathrm{D}}'(P_{\mathrm{s}})$为单调递增函数，式(16)也为单调递增函数，表明攻击节点在OBU传输功率P_{s}足够大的前提下能够检测合法的PC5通信。

检测到PC5通信后，攻击节点开始向PC5信道发起干扰攻击。从检测率$P_{\mathrm{D}}(P_{\mathrm{s}})$的微分方程中计算出检测阈值$E_{\mathrm{ps}}$：

$$E_{\mathrm{ps}} = \frac{2(g)^2}{h_{\mathrm{s}}^2h_1P_{\max}} \tag{18}$$

至此，得到了在OBU发射功率为P_{s}的情况下攻击节点的攻击策略及攻击节点能够检测到环境中PC5通信的阈值。利用博弈论的观点研究车辆的传输策略，在固定攻击节点传输策略P_{j}的条件下，OBU的综合目标函数$f(P_{\mathrm{s}})$的计算结果为：

$$f(P_{\mathrm{s}}) = \begin{cases} P_{\mathrm{T}}\left(\dfrac{P_{\mathrm{s}}h_{\mathrm{s}}}{g}-\dfrac{2P_{\mathrm{s}}h_{\mathrm{s}}}{h_1h_{\mathrm{j}}P_{\max}}-Y\right), 0\leqslant P_{\mathrm{s}}\leqslant E_{\mathrm{ps}} \\ \sqrt{\dfrac{2P_{\mathrm{T}}}{h_1P_{\max}}}\sqrt{P_{\mathrm{s}}P_{\mathrm{D}}(P_{\mathrm{s}})\left[P_{\mathrm{T}}P_{\mathrm{D}}(P_{\mathrm{s}})+(1-P_{\mathrm{T}})P_{\mathrm{F}}\right]}+ \\ \dfrac{P_{\mathrm{T}}h_{\mathrm{s}}}{g}\cdot P_{\mathrm{s}}(1-P_{\mathrm{D}}(P_{\mathrm{s}}))-\dfrac{2h_{\mathrm{s}}P_{\mathrm{T}}}{h_1h_{\mathrm{j}}P_{\max}}P_{\mathrm{s}}, E_{\mathrm{ps}}\leqslant P_{\mathrm{s}} \end{cases} \tag{19}$$

一次博弈过程如图3所示。首先固定车辆发射功率，研究攻击节点，即设P_{s}一定，计算P_{j}与P_{s}的关系。通过$f(P_{\mathrm{j}})$取得最大值，得到攻击节点的最优攻击策略P_{j}。而后将攻击节点的最优传输策略P_{j}带入$f(P_{\mathrm{s}})$，得到仅关于P_{s}的目标函数。

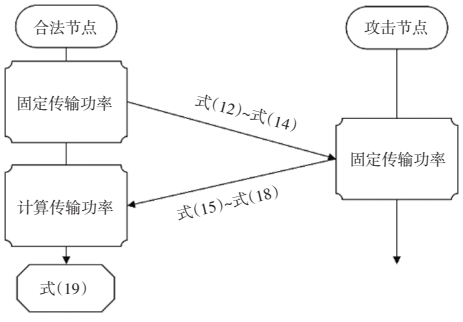

图3　一次博弈过程

根据实际g与$P_{\max}$的关系，当$0<P_{\mathrm{s}}<E_{\mathrm{ps}}$时，$f(P_{\mathrm{s}})$为关于$P_{\mathrm{s}}$的单调递增函数，取$P_{\mathrm{s}}=E_{\mathrm{ps}}$时得到$f(P_{\mathrm{s}})$的最大值。当$E_{\mathrm{ps}}<P_{\mathrm{s}}$时，首先分析$f(P_{\mathrm{s}})$的单调性。计算$f(P_{\mathrm{s}})$的一阶导数，结果为：

$$\begin{aligned} &\frac{\partial f_{\mathrm{T}}}{\partial P_{\mathrm{s}}} = \\ &\frac{\sqrt{\dfrac{2P_{\mathrm{T}}h_{\mathrm{s}}}{h_{\mathrm{s}}h_1P_{\max}}}\left\{P_{\mathrm{D}}(P_{\mathrm{s}})\left[P_{\mathrm{T}}P_{\mathrm{D}}(P_{\mathrm{s}})+(1-P_{\mathrm{T}})P_{\mathrm{F}}\right]+P_{\mathrm{s}}P_{\mathrm{D}}'(P_{\mathrm{s}})\right\}}{2\sqrt{P_{\mathrm{s}}P_{\mathrm{D}}(P_{\mathrm{s}})\left[P_{\mathrm{T}}P_{\mathrm{D}}(P_{\mathrm{s}})+(1-P_{\mathrm{T}})P_{\mathrm{F}}\right]}}+ \\ &\frac{\sqrt{\dfrac{2P_{\mathrm{T}}h_{\mathrm{s}}}{h_{\mathrm{s}}h_1P_{\max}}}(1-P_{\mathrm{T}})P_{\mathrm{F}}+P_{\mathrm{T}}P_{\mathrm{D}}(P_{\mathrm{s}})P_{\mathrm{D}}'(P_{\mathrm{s}})}{2\sqrt{P_{\mathrm{s}}P_{\mathrm{D}}(P_{\mathrm{s}})\left[P_{\mathrm{T}}P_{\mathrm{D}}(P_{\mathrm{s}})+(1-P_{\mathrm{T}})P_{\mathrm{F}}\right]}}+ \\ &\frac{P_{\mathrm{T}}h_{\mathrm{s}}}{g}(1-P_{\mathrm{D}}(P_{\mathrm{s}}))-\frac{P_{\mathrm{T}}h_{\mathrm{s}}}{g}P_{\mathrm{s}}P_{\mathrm{D}}'(P_{\mathrm{s}})-\frac{2P_{\mathrm{T}}h_{\mathrm{s}}}{h_{\mathrm{s}}h_1P_{\max}} \end{aligned} \tag{20}$$

同样，通过研究$f(P_{\mathrm{s}})$的微分，分析得到攻击场景下合法车联网节点的传输策略。首先根据$f(P_{\mathrm{s}})$得到$f(E_{\mathrm{ps}})$，

以该点作为车联网节点传输功率的函数分界点，然后计算$f(0)$、$f'(0)$、$f'(E_{ps})$、$f(\infty)$、$f'(\infty)$，并通过多点微分得到函数的单调性关系：

$$\begin{cases}\lim_{P_s\to 0} f(P_s)=-YP_T\\ \lim_{P_s\to 0} f'(P_s)=\infty\\ \lim f'(E_{ps})>0\\ \lim_{P_s\to\infty} f(P_s)=-\infty\\ \lim_{P_s\to\infty} f(P_s)<0\end{cases} \tag{21}$$

在$0<P_s<E_{ps}$区间，$f(P_s)$为单调递增函数，在$E_{ps}<P_s$区间，根据式(21)，$f(P_s)$的单调性不唯一。利用式(20)计算出所有使$f'(P_s)=0$的点，即极值点a_1、a_2、a_3、……、a_n。比较$f(E_{ps})$、$f(a_1)$、$f(a_2)$、$f(a_3)$、……、$f(a_n)$，得到极值点后，通过比较极值点的大小，取得范围内的最大值及对应发射功率，即为当前最优的函数值和发射功率。在整个干扰攻击过程中，OBU按照$f(P_s)$动态调整信号发射功率。本文以此提高传输信噪比，可降低通信延时，缓和干扰攻击。

3 试验验证

通过带入环境参数分析$f(P_s)$的函数特征，即分析延时攻击场景下车辆的传输策略。设环境中固有噪声功率为30 dBm，天线的最大传输功率P_{max}=30 dBm，车辆发射信号通信的概率P_T=0.8，攻击阶段漏检概率P_F=0.1，时间与采样频率的乘积tf_s=2，天线(信道)增益h_s、h_i、h_j均为6 dBi，并假设函数$f(E_{ps})$分段点，取E_{ps}=10 dBm。仿真结果如图4所示。

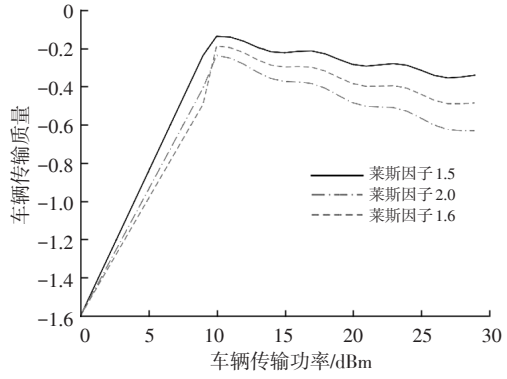

图4 不同莱斯因子下车辆的传输策略

随着环境中莱斯因子的变化，$f(P_s)$在微分中的表现略微差异。环境中莱斯因子越大，目标函数$f(P_s)$越小，但$f(P_s)$的微分趋势相同。莱斯因子影响了应用环境中车联网RSU与其他OBU的通信，即影响了噪声莱斯衰落后的信噪比。

对比应用环境中使用$f(P_s)$传输策略和以恒定功率通信的信噪比。环境中莱斯因子始终取2。构建应用环境中的模型：

$$X_{P_j}=\frac{P_s}{\partial P_j+g+Y} \tag{22}$$

式中，X_{Pj}为在攻击节点的攻击功率为P_j条件下合法车联网节点的信噪比；补偿系数∂=0.9用于补偿由攻击节点到合法车联网节点之间距离带来的噪声损失。

此时的检测阈值E_{ps}约为0.4。设定车联网节点V2X传输通信的功率为15 dBm，结果如图5所示。

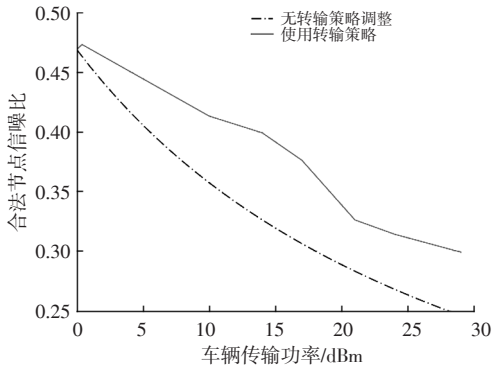

图5 信噪比随攻击节点功率的变化趋势

仿真结果表明，本文设计的基于信噪比的延时攻击防御方案通过动态调整发射功率，使得合法节点在攻击节点的传输功率线性增大时保持了较高的水平，在一定程度上缓解了延时攻击。

借助V2X实体设备开展试验，设备布置如图6所示。

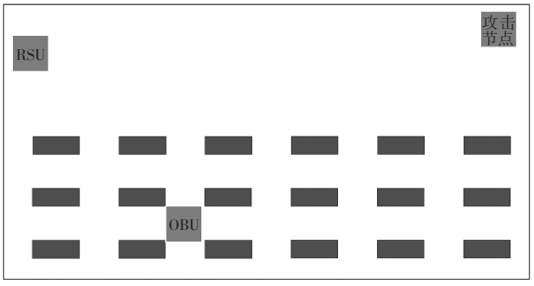

图6 试验设备布置

所使用的V2X设备OBU、RSU如图7、图8所示，天线增益为6~8 dB，驻波比不超过2。

图7 OBU设备

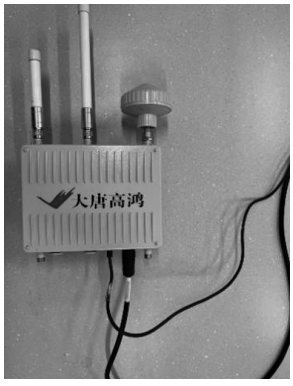

图8　RSU设备

借助场景仿真软件，构建可视化仿真环境如图9所示，试验中可量化参数如表1所示。

图9　可视化仿真环境

表1　试验参数

序号	参数类别	数值
1	最大发射功率/dBm	−65
2	环境噪声/dBm	−90
3	天线增益/dBm	7±1
4	实验室长度/m	30
5	实验室宽度/m	23
6	攻击节点攻击噪声功率/dBm	−100~−80

首先在未开启攻击时查看OBU传输信号与干扰加噪声比（Signal to Interference plus Noise Ratio，SINR），结果如图10所示。

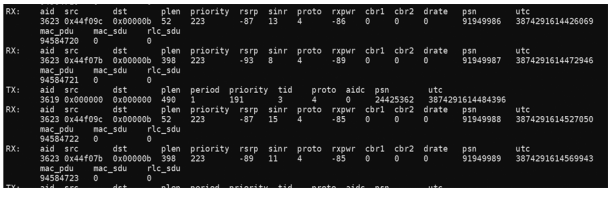

图10　OBU通信电气信息

待信噪比平稳后，其数值约为16。通过逐渐增大攻击节点功率分析信噪比变化，结果如图11所示。

由以上试验结果可知，在攻击节点功率一定的情况下，OBU按照$f(P_s)$动态调整信号发射功率较未使用动态策略的OBU具有更大的信噪比。调整策略基于车联网车辆与车辆（Vehicle to Vehicle，V2V）通信场景下的发射功率要求，并非简单提升发射功率，保证了使用此防护方案的OBU或RSU对其他车联网单元的额外干扰保持在较低水平。

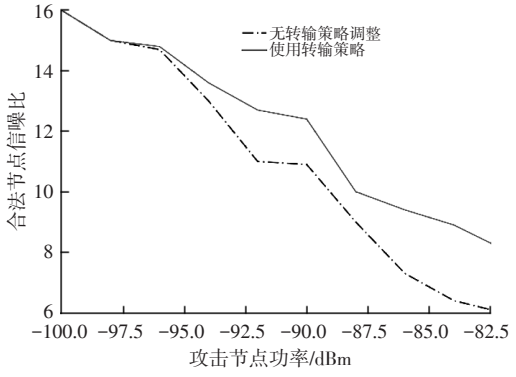

图11　信噪比随攻击节点功率变化趋势

4　结束语

本文研究了车联网场景下PC5信道的延时攻击防护技术，使用信噪比为指标，利用博弈论分析了V2X车联网节点传输功率与攻击者干扰攻击功率之间的关系。考虑攻击节点干扰模型，通过一次博弈，根据干扰攻击的变化改变OBU及RSU的传输功率。最后通过仿真与V2X设备试验证明了为抵御干扰攻击，综合考虑发射功率、信噪比、检测概率并得到合法节点的传输策略能够保障V2X通信的安全性。该防护方案可以缓解因环境中噪声干扰增多而导致通信信噪比快速下降的问题，进而保证了业务通信的延时要求。

参　考　文　献

[1] 李哲. 基于V2X的无线通信网络性能测量与评价[D]. 重庆: 重庆邮电大学, 2018.
LI Z. Performance Measurement and Evaluation of Wireless Communication Network Based on V2X[D]. Chongqing: Chongqing University of Posts and Telecommunications, 2018.

[2] WANG J, SHAO Y M, GE Y M, et al. A Survey of Vehicle to Everything (V2X) Testing[J]. Sensors, 2019, 19(2): 334.

[3] SHIMIZU T, CHENG B, LU H, et al. Comparative Analysis of DSRC and LTE-V2X PC5 Mode 4 with SAE Congestion Control[C]// 2020 IEEE Vehicular Networking Conference (VNC). New York, NY, USA: IEEE, 2020: 1-8.

[4] LIANG H J, WEINAND A, HAN B, et al. Multi-RATs Support to Improve V2X Communication[C]// 2018 IEEE Wireless Communications and Networking Conference (WCNC). Barcelona, Spain: IEEE, 2018: 1-6.

[5] PETIT J, SHLADOVER S E. Potential Cyberattacks on

Automated Vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(2): 546-556.

[6] PARKINSON S, WARD P, WILSON K, et al. Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(11): 2898-2915.

[7] RABIEH K, MAHMOUD M M E A, GUO T N, et al. Cross-Layer Scheme for Detecting Large-Scale Colluding Sybil Attack in Vanets[C]// IEEE International Conference on Communications (ICC). London, UK: IEEE, 2015.

[8] MEJRI M N, BEN-OTHMAN J, HAMDI M. Survey on Vanet Security Challenges and Possible Cryptographic Solutions[J]. Vehicular Communications, 2014, 1(2): 53-66.

[9] FAKKORIAN S A A, SWINDLEHURST A L. Solutions for the MIMO Gaussian Wiretap Channel with a Cooperative Jammer[J]. IEEE Transactions Signal Processing, 2011, 59 (10): 5013-5022.

[10] MOON J, LEE H, SONG C, et al. Secrecy Outage Minimization for Wireless Powered Communication Networks with an Energy Har-Vesting Jammer[C]// IEEE Global Communications Conference. Washington D.C., US: IEEE, 2016.

[11] TANG X, REN P Y, WANG Y C, et al. Securing Wireless Transmission Against Reactive Jamming: A Stackelberg Game Frame-Work[C]// IEEE Global Communications Conference. San Diego, CA, USA: IEEE, 2015.

[12] AMURU S, DHILLON H S, BUEHRER R M. On Jamming Against Wireless Networks[J]. IEEE Transactions on Wireless Communications, 2017, 16(1): 412-428.

[13] XUAN Y, SHEN Y, NGUYEN N P, et al. A Trigger Identification Service for Defending Reactive Jammers in WSN[J]. IEEE Transactions on Mobile Computing, 2012, 11 (5): 793-806.

[14] YAN Q B, ZENG H C, JIANG T T, et al. Jamming Resilient Communication Using MIMO Interference Cancellation[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(7): 1486-1499.

[15] 陈萍，熊蔚明. 一种可用于莱斯衰落信道的信噪比估计算法[J]. 东南大学学报(自然科学版)，2017, 47(2): 209-214.
CHEN P, XIONG W M. A Signal-to-Noise Ratio Estimation Algorithm For Rice Fading Channel[J]. Journal of Southeast University (Natural Science Edition), 2017, 47 (2): 209-214.

[16] 吴晓鸽，于龙海，凌捷. 基于信噪比的延时攻击防御方法研究[J]. 计算机应用与软件，2022, 39(5): 330-335.
WU X L, YU L H, LING J. Research on Delay Attack Protection Based on Signal-to-Noise Ratio[J]. Computer Applications and Software, 2022, 39(5): 330-335.

（责任编辑　斛　畔）

修改稿收到日期为2022年11月23日。