DOI:10. 3969/j. issn. 1674-1951. 2021. 02. 003

G3-PLC中MAC层动态信任评价机制研究

Research on dynamic trust evaluation mechanism on MAC layer in G3-PLC

董重重[1],谢玮[1],孙秉宇[1],简子倪[2],蒋究[2*],王先培[2]
DONG Chongchong[1], XIE Wei[1], SUN Bingyu[1], JIAN Zini[2], JIANG Jiu[2*], WANG Xianpei[2]

(1.国网湖北省电力公司计量中心,武汉 430080; 2.武汉大学 电子信息学院,武汉 430072)
(1.State Grid Hubei Electric Power Company Metering Center, Wuhan 430080, China;
2. Electronic Information School, Wuhan University, Wuhan 430072, China)

摘 要:G3-PLC是目前应用最为广泛的电力线通信标准协议之一,适用于智能电网的抄表、监测等传输数据速度要求不高的场合。为保障G3标准下电力线载波通信安全,以无线通信安全技术标准为依据,在媒体接入控制(MAC)层已有的MAC通信层和6LoWPAN安全认证层的基础上增加MAC感知子层,并建立动态信任评价机制模型,实现对用户频谱资源的合理分配。该信任机制基于客户端用户行为进行评价,利用强化学习方法,采用信任值升降作为奖惩制度,以信任值为判据实现服务端对客户端频谱资源的分配,确保每个感知用户在通信过程中与信誉高的节点融合并降低恶意用户的信任值,从而进行正确频谱感知,抑制分配不信任用户频谱资源,最终将不信任用户剔除出整个网络。

关键词:G3-PLC;无线通信;智能电网;媒体接入控制层;频谱资源;信任评价机制;强化学习;客户端;服务端
中图分类号:TN 915.85:TM 73 **文献标志码**:A **文章编号**:1674-1951(2021)02-0015-07

Abstract: G3-PLC is one of the most widely used power line communication standard protocols. It is suitable for applications which make moderate requests on data transmission speed, such as meter reading and smart grid monitoring. In order to ensure the security of power line carrier communication under the standard G3, an extra MAC sensing sublayer was added on the existing MAC communication layer and 6LoWPAN security authentication layer of Media Access Control (MAC) layer, in compliance with the wireless communication security technology standard. And a dynamic trust evaluation mechanism model was constructed to make reasonable allocation of user spectrum resources. The trust mechanism makes evaluation according to users' behavior by reinforcement learning. Taking trust value as the reward and punishment system, the trust value is used as the criterion to distribute spectrum resources between clients. Ensuring that each perception client can be fused with high-reputation nodes in the process of communication, the trust value of malicious users will be reduced. The method can perform correct spectrum sensing, suppress the spectrum resources allocated to malicious users, and finally remove malicious users away from the entire network.

Keywords: G3-PLC; wireless communication; smart grid; MAC layer; spectrum resources; trust evaluation model; reinforcement learning; client; server

0 引言

电力线载波通信是利用已铺设好的电力线网络进行信息传输的一种通信方式[1],由于不需要额外的通信线路,具有较高的经济性和便捷性[2-3]。随着智能电网理念的提出与发展,电力通信技术逐步受到重视。受制于早期电力线建设的局限性,传统的载波通信技术稳定性较差,系统容易受到干扰,通信效率与可靠性较低[4-5]。如何提高载波通信对抗阻抗匹配、频率选择衰落等影响因素的能力,是相关领域研究的热点问题[6]。

G3-PLC属于窄带电力线载波通信,在智能电网抄表、监测等传输数据速度要求不高的场合得到了广泛应用[7],其物理层采用OFDM调制技术与信道纠错编码结合的方式,使得数据传输过程相较于传统方法更为可靠[8-9];同时,G3-PLC标准信号帧结构完整,受到主流国际电表厂商的青睐,符合我国低压电网通信频带的要求[10-12]:因此,本文以G3标准电力线载波通信为典型,研究电力线载波通信安全技术。

收稿日期:2020-07-10;**修回日期**:2021-01-25
基金项目:国家自然科学基金项目(51707135)

1 MAC感知层功能结构

在G3-PLC标准中，媒体接入控制（MAC）层基于低速无线个人局域网的IEEE 802.15.4标准制定，采用了载波侦听多点接入/冲突避免（CSMA/CA）以及自动重传请求（ARQ）机制，可以实现对误差的检测，使得数据传输过程更为可靠[13-14]。

针对MAC协议，国内外学者都对其优化进行了相关研究。文献[15]设计了一种基于时间段的新MAC协议，以提高电力线通信（PLC）网络数据传输效率和稳定性；文献[16]提出了一种增强MAC协议，在链路层级别融合协作协议与数据包校正技术，提高了PLC系统数据通信的可靠性；文献[17]提出了一种适用于低压电力线通信中有限负载网格（Mesh）网络的自适应p-CSMA MAC效率优化方法，充分利用PLC有限的带宽资源，提高了有限负载Mesh网络的MAC效率性能。本文针对G3-PLC协议MAC层实现感知子层与动态评价机制的构建，以提高数据传输的稳定性与可靠性。

认知无线电技术在时域、频域和空域上采用机会式频谱接入[18]，其关键在于可以动态访问处于空闲状态的授权频谱，利用频谱感知等方法确定授权频段状态信息，使得用户获得额外的频谱利用机会，提高频谱利用率[19]。基于此思想，将MAC层设计为3个子层：负责通信的MAC子层、提供感知能力的MAC感知子层以及提供消息认证等功能的6LoWPAN安全层。图1为感知子层的主要结构：首先，感知子层应根据已接收的信息对频谱进行判断，并依据决策功能判断接收数据是否存在异常；随后进行认证、授权等相关步骤，获得可以实现通信的空闲频谱，实现频谱的合理安全分配，防止干扰授权客户的通信，使得用户获得额外的频谱利用机会，提高频谱利用率[20-22]。

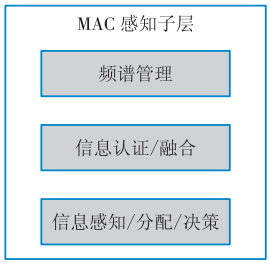

图1 MAC感知子层结构

Fig. 1 Structure of the MAC sensing sublayer

MAC层安全机制的构建以用户的信任程度为基础，信任程度值由感知子层分析客户端频谱数据正确率而生成。信任值良好的用户保留使用频谱资源的权利，代表用户行为与网络利益的一致程度；出现攻击现象的用户将被降低信任值，一旦信任值低于标准，该用户将被判别为不信任用户，限制其对频谱资源的使用，甚至从网络中剔除。

2 信任评价模型

在信任评价模型中，用户信任值的综合评价由直接信任值评价和间接信任值评价2个方面组成。其中，直接信任值的计算依据是直接行为（如是否发送正确的频谱数据），衡量该用户过往的数据传输行为是否与网络整体利益保持一致，并不断被更新；间接信任值由与此用户产生过信息传输的最后服务器端提供。对直接信任值和间接信任值进行加权相加，可以得到综合的信任值评价[23]，以此为依据对用户进行分类，限制恶意用户，合理分配频谱资源。

2.1 信任值计算

设定评价模型中执行评价的服务器为S_i，被评价客户端为C_j，评价信任值$f(i,j)$在区间[0,1]之间取值。由于直接信任值计算基于用户的实时行为，则$f(i,j)$是关于时间行为的离散函数。在某时间段内共有n个行为片段$\left[t_1,t_2,\cdots,t_n\right]$，在第$k$个行为片段内，行为记录有$N_{t_k}$个，则有直接信任值$D_{ij}^{t_k}$

$$D_{ij}^{t_k}=\frac{\sum_{m=1}^{N_{t_k}}f(i,j)}{N_{t_k}}。\tag{1}$$

在第m个时间间隔中，评价信任值为

$$f_m(i,j)=b_{ij}+a_{ij}u_{ij}=\frac{r+1}{r+s+2},\tag{2}$$

式中：r表示成功；s表示失败。表示在第m个间隔内，客户端给服务端发送正确频谱数据次数为r，错误频谱数据次数为s。

由于信任值评价应随着时间的推移而动态变化，且时间上相对接近的行为对评价结果的影响应该更加显著，所以在评价公式中引入衰减指标

$$f_k=\varphi^{n-k},\tag{3}$$

式中：φ为衰减因子，$0<\varphi<1$；k为小于n的正整数。

引入衰减因子后，由式(1)可以推导出

$$D_{ij}=\frac{\sum_{k=1}^{n}f_k\times D_{ij}^{t_k}}{\sum_{k=1}^{n}f_k}。\tag{4}$$

使用式(4)完成对用户信任值的量化，设定每个用户的初始信任值均为0.5，直接信任值随用户行为变化。

除了直接信任值，还需要从其他服务器得到用户的间接信任值，I_n代表本服务器从其他服务器获取的推荐信任值评价，I_f为上一服务器对该用户的

信任评价

$$I_n = I_f 。 \tag{5}$$

若该用户未与其他服务器进行过通信，则将初始间接信任值设置为 0.5。

2.2　权重计算

信任评价由直接信任值和间接信任值加权相加组成，设直接信任值权重为 α、间接信任值权重为 β，则有

$$\alpha = \frac{f_c}{f_c + f_f}, \tag{6}$$

$$\beta = \frac{f_f}{f_c + f_f}, \tag{7}$$

式中：f_c 为置信因子，表现为综合信任值对直接信任值的重视程度；f_f 为反馈因子，表现为综合信任值对间接信任值的重视程度。

假设在当前时间段内，客户端向服务器发送频谱的总次数为 N_s，服务器判定发送错误的次数为 n_w，则有

$$f_c = 1 - \lambda^{\frac{N_s - n_w}{N_s + \gamma}}, \tag{8}$$

式中：λ 为置信因子 f_c 的衰减速度，$0<\lambda<1$；γ 为置信因子 f_c 的增长速度，γ 值越大则 f_c 增长越快。服务器可以根据需要调节 λ 与 γ 设定自信因子随客户端行为变化的趋势。

同样，对于反馈因子 f_f 有公式

$$f_f = 1 - \kappa^{\frac{N_c - n_r}{N_c + \sigma}}, \tag{9}$$

式中：N_c 为被评估客户端与其他服务器进行通信的次数；n_r 为服务器拒绝与此客户端通信的次数；κ 为 f_f 的衰减速度，$0<\kappa<1$；σ 为 f_f 的增长速度。

则当前行为片段内，信任综合评价值 C_{ij} 为

$$C_{ij} = \alpha D_{ij} + \beta I_n 。 \tag{10}$$

2.3　信任值更新

通信过程中系统信任值需要实时更新，因此将客户端与服务器的信任值按时间周期进行计算更新，同时将上一时间周期的信任值评估结果作为参考进行评估。设当前信任值为 $C_{t_{i+1}}$、上一时间周期的历史信任值为 C_{t_i}，则加权计算综合信任值为

$$C_{t_{i+1}} = w_{i_1} C_{t_{i+1}} + w_{i_2} C_{t_i}, \tag{11}$$

式中：w_{i_1}，w_{i_2} 分别为当前评价值与历史评价值的权值，$w_{i_1} + w_{i_2} = 1$。

由于实际应用中客户端的当前行为对整体评价影响更大，而历史评价值应随时间衰减，故将其权重设定为时间衰减函数，即

$$w_{i_2} = \eta^{t_{i+1} - t_i}, \tag{12}$$

式中：$t_{i+1} - t_i$ 为 2 次评价之间的时间周期；η 为时间衰减因子，$0<\eta<1$，η 值越大，则历史信任评价结果对整体评价的影响越大，在评价过程中需要以当前客户端行为为主，故 η 应设为较小值。

3　基于强化学习的服务端资源分配

当多个客户端请求频谱资源分配时，利用强化学习机制对信誉高的客户端优先分配频谱资源。在动态信任评价中，评价机制与感知循环有 2 个交换。

（1）服务端从信任值高的客户端收集频谱感知数据，将这些感知数据进行分析并决策，服务端将决策结果发送给所有客户端。服务端将决策结果与客户端发送的感知数据进行对比，从而判定客户端感知结果是否正确，依据判定结果对信任值进行更新。如果比较结果相同，则该客户端直接信任值增加，否则，直接信任值减少。

（2）当服务端采用强化学习方法对周围客户端进行频谱资源分配时，将客户端分为信任客户端、不确定客户端和不信任客户端，对信任客户端进行频谱分配，对不确定客户端依照至信任客户端路径随机分配，对不信任客户端不分配频谱资源。

强化学习属于无监督机器学习[24]，通过与环境的交互来采取相应的行为（如图 2 所示），包括环境和智能体（Agent）2 个部分，其整个思想为奖惩机制：Agent 的某个行为结果发生之后，环境表明该行为对达到最初目标有效，就对这种行为进行奖励，Agent 在了解这种行为可以获得奖励之后，就会按照奖励的多少执行奖励最高的行为从而获得最多的奖励，这样周而复始，不断学习，最终学习到最优的行为方式。

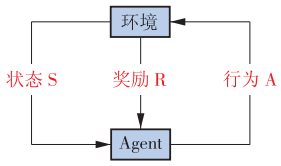

图 2　强化学习结构

Fig. 2　Process of reinforcement learning

强化学习分为多种，Q-Learning 由于使用效果好、适应能力强且所需要的先验知识相对较少而得到广泛应用[25]。Q-Learning 包含状态、行为和奖励 3 个模块：状态表示 Agent 所在的环境集合，Agent 之后的行为被该环境集合所决定；行为表示的是 Agent 在当前状态下以及选择不同奖励后发生的行为；奖励则为在执行该行为而得到的奖励，奖励有正有负。利用 Q 函数对其不同行为进行量化并评估

$$Q_{t+1}(s_t,a_t)\leftarrow(1-\xi)Q_t(s_t,a_t)+\xi[r_{t+1}(s_{t+1})+\delta\max_{a\in A}Q_t(s_{t+1},a)],\tag{13}$$

式中：$r_{t+1}(s_{t+1})$为 Agent 在 t 时刻所处状态对应的奖励；$\delta\max_{a\in A}Q_t(s_{t+1},a)$为 Agent 所未发生行为中评估奖励最大值函数；ξ为学习速率，表示一次学习对整个状态值的影响；δ为折扣因子，表示对所未发生行为的奖励值的折扣；a为学习过程中的行为。

由于强化学习对最大奖励值行为不断地学习，效益高的策略会不断加强，$Q_t(s_t,a_t)$值会越来越大，Agent 找到最优策略，此时 $Q_t(s_t,a_t)$收敛，达到最大值

$$V_t(s_t)=\max_{a_i\in A}Q_t(s_t,a_t)。\tag{14}$$

由于整个信任模型基于强化学习，其信任值是随时波动的，故需要对其量化，在本文动态评价机制中，将信任值分为不同区间，包括可信任区间、不确定区间和不可信任区间，各个区间的值分别设为(0.6,1.0]，(0.4,0.6]，(0,0.4]。服务端从自身节点出发，向周围未分配频谱资源的客户端分配频谱资源，依据信任值进行设置，信任值为(0.6,1.0]的客户端设置为1，信任值为(0.4,0.6]的客户端设置为0，信任值为(0,0.4]的客户端设置为-1，以此建立模型；服务端初始值设为0，由服务端节点出发，当服务端节点值收敛时，以服务端所途径路线分配频谱资源，从而达到对不信任客户端不分配频谱资源目的。

4 动态信任评价模型与频谱资源分配仿真

4.1 信任值计算

搭建评价模型并利用Matlab联合Python进行仿真，包括11个客户端和1个服务端，客户端包含好的用户、自私用户、缺陷用户以及恶意用户，客户端的初始信任值由推荐信任值确定，第1次接入为0.5，服务端初始值为0。参数设置为：φ=0.4，λ=0.4，κ=0.4，η=0.3，γ=2，σ=2，Δt=20 s。

计算每个客户端即用户的信任值，仿真包括以下2个方面。

(1)通过客户端信任值更新过程表现该评价机制的作用。客户端用户包括好的用户、自私的用户、恶意用户以及有缺陷的用户。自私的用户也是合法用户，由于占用更多的频谱导致其他用户的频谱使用无法满足；恶意用户为了非法目的给服务端发送错误的频谱数据，从而误导服务端的操作；当有缺陷用户的设备出现故障，或由于其他干扰导致其发送错误的频谱数据给服务端时，信任值下降，但故障消除后该属性用户信任值会逐渐恢复上升。根据客户端信任值波动曲线识别出用户的不同属性，如图3所示。为方便对服务端进行频谱资源分配，将用户信任值分为3种状态：(0.6,1.0]，可信状态；(0.4,0.6]，不确定状态；(0,0.4]，不可信状态，对恶意用户进行频谱资源分配压制，并最终将恶意用户拒绝于网络之外。

整个试验过程中采用集中式频谱感知方法，不同的网络攻击力度下，客户端发生的错误概率仿真结果见表1。

表1 网络攻击下客户端错误概率

Tab. 1 Client error probability under network attacks

攻击力度	客户端编号				
	1—3	4	5—9	10	11
0	0	0	0	0	0
0.1	0	0	0	0	0.1
0.2	0	0.1	0	0	0.1
0.3	0	0.1	0.1	0	0.1
0.4	0	0.1	0.1	0	0.2
0.5	0	0.2	0.1	0	0.2
0.6	0	0.2	0.1	0	0.3
0.7	0	0.2	0.2	0	0.3
0.8	0.1	0.2	0.2	0	0.3
0.9	0.1	0.2	0.2	0	0.4
1.0	0.1	0.2	0.2	0	0.5

(2)仿真不同行为模式对频谱资源分配的影响。行为模式包括正常行为及非正常行为，非正常行为包括2种：1)假警报攻击，当一个频谱处于空闲状态时，客户端发送数据表示该频谱被占用；2)完成错误检测攻击，与1)相反，一个频谱被占有，而客户端发送的数据表明该频谱空闲，从而导致发生错误，影响客户端通信。

4.2 信任值更新过程

依据使用行为，用户可以被分为好用户、自私用户、故障用户以及恶意用户进行信任值更新(如图3所示)，为了便于实现频谱资源分配，这4类用户最终可以根据信任值被分为可信用户、不确定用户以及不可信用户，并由服务端进行相应的频谱资源管理。

在图3a中，好用户的信任值持续增加到1，图3b中自私用户在可信任阶段和不确定阶段波动，主要在不确定阶段，所以自私用户使用频谱的概率较低。图3c显示的是有故障用户，故障后发送错误的频谱数据导致其信任值下降，故障排除后如果信任

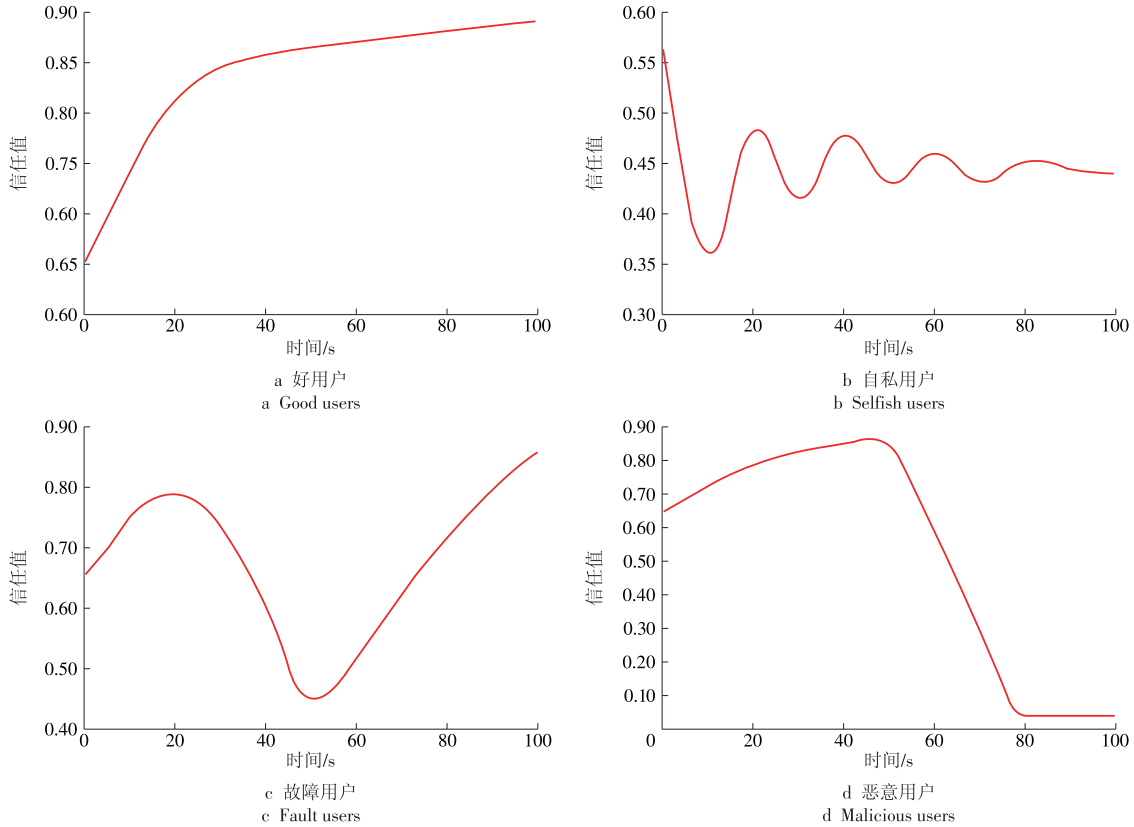

图 3　不同种类用户的信任值更新过程

Fig. 3　Trust re-evaluation process of different clients

值能够恢复至可信阶段,该用户还可以成为可信任用户,如果信任值难以恢复并下降至不可信状态,则该用户可能会被排除网络之外。图 3d 是一个恶意用户,忽略其历史的信任值,一旦频发错误的数据,其信任值降低到丢弃阶段。

4.3　服务端频谱资源分配

完成信任值更新后,服务端对其周围的客户端进行频谱资源分配,对 Mesh 网络结构[26]进行简化,建立模型。假设 10 个客户端有 1 个是信任用户,信任值为(0.6, 1.0],2 个恶意用户,信任值为(0, 0.4],其他 7 个客户端为不确定用户,信任值为(0.4, 0.6],为使服务端更高效地进行频谱资源仿真,从服务端出发,搜索网络中最短路径至信任值为 1 的客户端,并对沿途路径客户端进行资源分配,整个网络模型如图 4 所示。

如图 4 所示,10 为信任用户,4 和 11 为恶意用户,1 为服务端,每次从 1 出发,利用强化学习方法搜索整个网络,寻找到信任用户,分配频谱资源,为了最大效率分配频谱资源,对沿途不确定用户进行频谱资源分配。因此,服务端应寻找到达客户端的最短路径并进行频谱资源分配,避过恶意用户客户端,从而能够更高效地分配频谱资源并压制恶意用户对频谱资源的使用。

仿真参数中学习率和折扣因子分别为 0.3 和

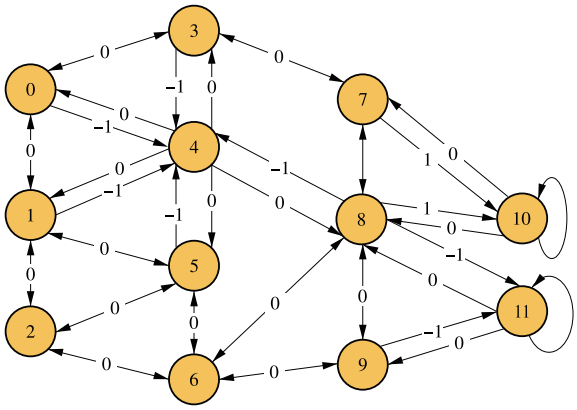

图 4　不同种类用户的信任值更新过程

Fig. 4　Process of updating trust value of different types of users

0.9,经过多次迭代后,其搜索路线被确定,即分配频谱资源客户端被确定。为更好地表示多次搜索后整个频谱资源的分配,每次迭代后将 Q 表中 1-0,1-2,1-4,1-5 和的平均值作为服务端的状态值 S,图 5、图 6 分别为迭代 100 次和 300 次后的服务端 S 值。

由图 5、图 6 可见,迭代 50 次左右后服务端 S 值收敛在 0.5 左右,说明整个服务端频谱资源分配路线规划趋于稳定,仿真结果显示,其路线为:1→2→6→8→10 或 1→5→6→8→10 或 1→0→3→7→10。由于网络模型较为简单,故存在多种路径选择,它们均为至信任用户客户端的最短路径,同时避开了

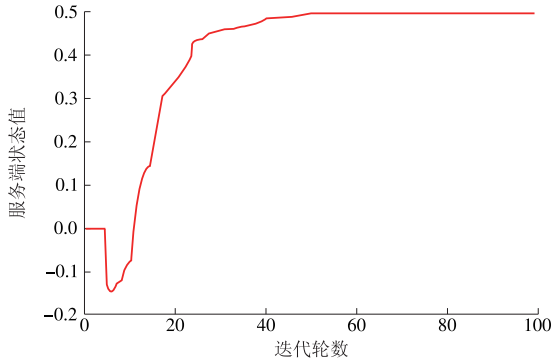

图 5 迭代 100 次后服务端 *S* 值

Fig. 5 *S* value on server after 100 iterations

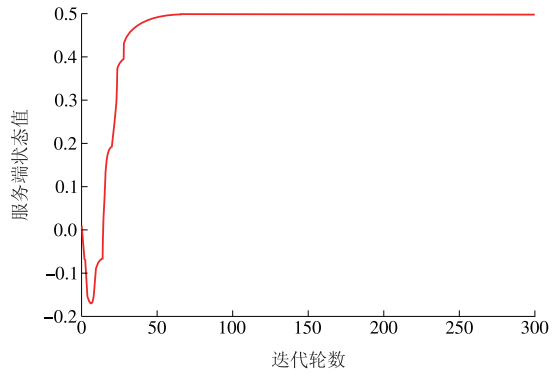

图 6 迭代 300 次后服务端 *S* 值

Fig. 6 *S* value on server after 300 iterations

恶意用户客户端，这与实际情况相符。在一段时间间隔后，客户端信任值更新，对服务端周围的客户端重新进行频谱资源分配，信任值低的恶意用户的频谱资源一直处于饥饿状态，信任值高的好用户的频谱资源一直处于饱和状态，而信任值不确定用户的频谱资源处于不确定的半饱和状态，从而达到压制恶意用户频谱资源以及更加有效分配频谱资源的目的。

拒绝服务攻击是恶意用户侵入网络进行攻击的主要方式之一，通过发送非法请求耗尽服务端资源，从而达到合法用户请求无法响应的目的。而采用动态信任评价机制建立客户端信任值模型，并对已建立的客户端信任值模型进行有目的的频谱资源分配，可以起到抵抗拒绝服务攻击的目的。

5 结论

本文中，服务端依据客户端一个时间间隔内发送的客户端频谱数据进行综合分析，从而更新客户端的信任值并建立动态信任评价机制模型。依据客户端信任值更新曲线，将客户端分为好用户、自私用户、故障用户以及恶意用户。为抵抗恶意用户可能通过耗尽服务端资源来进行攻击的行为（如拒绝服务攻击），利用已建立好的动态信任评价机制模型，依据信任值所在的区间，将客户端分为信任用户、不确定用户和不信任用户，通过强化学习方法，有目的地对不同属性的客户端分配频谱资源，从而压制恶意用户的频谱资源使用，最终将不信任用户剔除网络，起到保护整个网络安全的作用。

参考文献：

[1]耿旭. 基于电力线载波通信的远程自动抄表系统的研究[D]. 长春：吉林大学，2018.

[2]王艳，薛晨，焦彦军. 中压配电网 PLC 信道正反向传输特性分析[J]. 电力科学与技术学报，2020，35(3)：127-134.
WANG Yan，XUE Chen，JIAO Yan jun. Forward and backward transmission characteristics analysis of PLC channel in medium voltage distribution networks[J]. Journal of Electric Power Science and Technology，2020，35(3)：127-134.

[3]李艳，张安龙，郑曦. 配电网广域保护信息流建模与通信性能分析[J]. 电力科学与技术学报，2019，34(2)：53-60.
LI Yan，ZHANG Anlong，ZHENG Xi，Modeling and communication performance analysis of wide-area protection information flow in distribution network [J]. Journal of Electric Power Science and Technology，2019，34(2)：53-60.

[4]赵黎，焦晓露，张峰. 一种新的窄带电力线载波通信物理层模型[J]. 现代电子技术，2018，41(15)：6-9，15.
ZHAO Li，JIAO Xiaolu，ZHANG Feng. A new physical layer model of narrow-band power line carrier communication[J]. Modern Electronics Technique，2018，41(15)：6-9，15.

[5]杨鑫，徐刚，荀思超，等. 基于 McWiLL 无线宽带技术的县域电力通信网建设方案[J]. 电气技术，2016(5)：81-84.
YANG Xin，XU Gang，XUN Sichao，et al. County electric power communication network construction program based on McWiLL wireless broadband technology [J]. Electrical Engineering，2016(5)：81-84.

[6]周宇，张峰，刘艳. 基于嵌入式平台的 G3-PLC 系统设计与性能优化[J]. 通信技术，2020，53(5)：1163-1168.
ZHOU Yu，ZHANG Feng，LIU Yan. Design and performance optimization of G3-PLC system based on embedded platform[J]. Communications Technology，2020，53(5)：1163-1168.

[7]任会芬. 基于 G3-PLC 标准的低压电力线窄带通信系统研究[D]. 哈尔滨：哈尔滨工业大学，2013.

[8]MALEK M，KETEL D，HIRSCH H ，et al. Investigation of smart meters using G3 PLC[C]// International Symposium on Electromagnetic Compatibility，2016.

[9]BERT L D，D′ALESSANDRO S，TONELLO A M. MAC enhancements for G3-PLC home networks [C]// IEEE International Symposium on Power Line Communications & Its Applications，2013.

[10]黄增先,王进华.基于G3-PLC的RS译码器的设计与实现[J].微型机与应用,2016,35(17):68-71.
HUANG Zengxian, WANG Jinhua. Design and implementation of RS decoder based on G3-PLC [J]. Microcomputer & Its Applications, 2016,35(17):68-71.

[11]赵龙,胡正伟,谢志远.基于LDPC的改进G3-PLC物理层规范模型[J].电测与仪表,2018,55(10):19-23.
ZHAO Long, HU Zhengwei, XIE Zhiyuan. Physical layer specification model of improved G3-PLC based on LDPC [J]. Electrical Measurement & Instrumentation, 2018, 55 (10):19-23.

[12]刘晓胜,吴海涛,郑检,等.基于G3标准的窄带PLC通信方案设计[J].电气传动,2013,43(S1):123-127.
LIU Xiaosheng, WU Haitao, ZHENG Jian, et al. Design of narrow-band high speed power line communication system used in smart grid [J]. Electric Drive, 2013, 43 (S1):123-127.

[13]徐新雷,郭静波,王林川.电力线通信MAC层综述[J].电力信息化,2013,11(3):7-12.
XU Xinlei, GUO Jingbo, WANG Linchuan. Overview of MAC layer in power line communications [J]. Electric Power Information Technology, 2013,11(3):7-12.

[14]马国峰.G3-PLC开放式通信标准促进智能电网发展[J].今日电子,2012(6):39-44.
MA Guofeng. G3-PLC open communication standard promotes the development of smart grid [J]. Electronic Products, 2012(6):39-44.

[15]LIU X, LIU H, CUI Y , et al. A new MAC protocol design based on time period for PLC network[C]// 2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN), 2017.

[16]OLIVEIRA R M, VIEIRA A B, RIBEIRO M V. EPLC-CMAC: An enhanced cooperative MAC protocol for broadband PLC systems [J]. Computer Networks, 2019, 153(22):11-22.

[17]CUI Y, LIU X. Research on MAC efficiency for broadband PLC access network [C]// 2017 3rd IEEE International Conference on Control Science and Systems Engineering (ICCSSE), 2017.

[18]AXELL E, LEUS G, LARSSON E G, et al. Spectrum sensing for cognitive rad state-of-the-art and recent advances [J].IEEE Signal Processing Magazine, 2012 , 29 (3): 101 -116.

[19]陈思吉,王欣,申滨.一种基于支持向量机的认知无线电频谱感知方案[J].重庆邮电大学学报(自然科学版),2019,31(3):313-322.
CHEN Siji, WANG Xin, SHEN Bin. A support vector machine based spectrum sensing for cognitive radios [J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2019, 31 (3):313-322.

[20]TSIROPOULOS G , DOBRE O A , AHMED M H , et al. Radio resource allocation techniques for efficient spectrum access in cognitive radio networks [J]. IEEE Communications Surveys & Tutorials, 2016, 18 (1) : 824-847.

[21]MITOLA J I, MARUIRE G Q J. Cognitive radio: Making software radios more personal [J]. IEEE Personal Communications, 1999, 6(4): 13-18.

[22]ZHANG M B, WANG L W, FENG Y Q, et al. A fast spectrum sensing for OFDM based on adaptive thresholding [C]//2017 IEEE 2nd IEEEI Advanced Information Technology,Electronic and Automation Control Conference, 2017 : 25 - 26.

[23]TSIROPOULOS G I, DOBRE O A, Ahmed M H, et al. Radio resource allocation techniques for efficient spectrum access in cognitive radio networks [J]. IEEE Communications Surveys & Tutorials, 2016, 18 (1) : 824-847.

[24]张孟伯, 王伦文, 冯彦卿. 基于强化学习和共识融合的分布式协作频谱感知方法[J]. 系统工程与电子技术, 2019,41(3):486-492.
ZHANG Mengbo, WANG Lunwen, FENG Yanqing. Distributed cooperative spectrum sensing method based on reinforcement learning and consensus fusion [J]. Systems Engineering and Electronics, 2019,41(3):486-492.

[25]CHEN Z, QIU R C. Cooperative spectrum sensing using Q-Learning with experimental validation [C] //2011 Proceedings of IEEE Southeastcon, 2011 : 405 - 408.

[26]WANG Jihong, SHI Wenxiao, JIN Feng. On channel assignment for multicast in multi-radio multi-channel wireless mesh networks: A survey [J]. China Communications,2015,12(1):122-135.

(本文责编:刘芳)

作者简介:

董重重(1985—),男,湖北武汉人,工程师,硕士,从事软件工程、调度自动化工作(E-mail: 414396666@qq.com)。

蒋究*(1997—),男,湖北武汉人,在读硕士研究生,从事系统集成与故障诊断等方面的研究(E-mail:jiangjiu@whu.edu.cn)。

王先培(1962—),男,湖北武汉人,教授,博士生导师,从事电力系统可靠性分析、系统集成与故障诊断等方面的研究(E-mail:xpwang@whu.edu.cn)。