doi:10.11835/j.issn.1000-582X.2021.224

配电边缘物联网网络预警及自愈方案

李伟青[1],陈虹宇[2],赵瑞锋[3],胡春强[2]
(1. 广东电网有限责任公司 梅州供电局,广东 梅州 514199; 2. 重庆大学 大数据与软件学院,
重庆 401331; 3. 广东电网有限责任公司 电力调度控制中心,广州 510062)

摘要:配电物联网是电力物联网建设中的最后一个环节,由于具有供电路径短、负荷密度大等特点,保护和控制的难度很大,需要建立完善的配电网预警和自愈策略,形成运行方式灵活、故障预警及时、故障自愈完善的智能配电网。为此,文中提出了适用于配电物联网边缘网络固件的安全防御技术框架,对存在边缘设备中的各固件可靠性矩阵进行保护,边缘设备通过边缘服务器相互连接,形成了具备安全预警及自愈能力的配电边缘物联网技术方案。最后,通过不同环境下的模拟实验验证了文中方案的可行性。

关键词:人工智能;漏洞预警;配电物联网;电网自愈
中图分类号:TM76;TM73　　**文献标志码:**A　　**文章编号:**1000-582X(2023)08-011-09

Artificial intelligence-based early warning and self-healing technology for distribution edge IoT networks

LI Weiqing[1], *CHEN Hongyu*[2], *ZHAO Ruifeng*[3], *HU Chunqiang*[2]
(1. Meizhou Power Supply Bureau of Guangdong Power Grid Co., Ltd., Meizhou, Guangdong 514199, P. R. China; 2. School of Big Data and Software Engineering, Chongqing University, Chongqing 401331, P. R. China; 3. Electric Power Dispatching and Control Center, Guangdong Power Grid Company Ltd., Guangzhou 510062, P. R. China)

Abstract: The distribution of IoT (Internet of Things) is the last link in the construction of ubiquitous power IoT. It possesses characteristics such as short power supply path and high load density, which bring about significant challenges in terms of protection and control. To address these challenges, the establishment of an early warning and self-healing strategy for the distribution network is crucial, enabling the formation of a smart distribution network with flexible operation mode, timely fault warning and perfect fault self-healing. This paper proposes a security defense technology framework applicable to the firmware of the distribution IoT edge network. The framework protects the reliability matrix of each firmware present in the edge devices, while the edge devices are interconnected through the edge servers, forming a technical solution for distribution edge IoT that incorporates security warning and self-healing capabilities. Finally, the feasibility of this scheme is verified by simulation experiments conducted under different environmental conditions.

Keywords: artificial intelligence; vulnerability alert; distribution IoT; grid self-healing

收稿日期:2021-11-15　　**网络出版日期:**2022-01-11
基金项目:国家自然科学基金资助项目(62072065);南方电网公司科技项目(GDKJXM20198151)。
Supported by National Natural Science Foundation of China (62072065), and Science and Technology Projects of China Southern Power Grid (GDKJXM20198151).

作者简介:李伟青(1986—),男,硕士,高级工程师,主要从事电力物联网研究,(E-mail) mzautolwq@163.com。
通信作者:胡春强,男,研究员,博士生导师,(E-mail)chu@cqu.edu.cn。

随着经济的不断发展，企业和用户对电力系统的供电水平的要求不断提升，电力系统的控制与保护也越发复杂。配电物联网作为电力生产和供应的最后一个环节，直接面向用户，是连接电力生产和用电用户的桥梁，影响着供电安全和可靠性。由于配电网具有供电路径短、负荷密度大等特点，保护和控制的难度很大，因此迫切需要建立完善的配电网预警和自愈策略，以此形成运行方式灵活、故障预警及时、故障自愈完善的智能配电网。如何在风险来临之前及时预警，在危机发生的情况下防止事故的连锁反应，已成为了当前研究的热点问题[1-3]。

配电物联网固件是配电物联网设备的基础使能软件，其中存在的安全缺陷是配电物联网设备遭受攻击的根本原因之一。固件如果身处不安全的环境中，其固件缺陷一旦被恶意利用，轻则使设备宕机，重则威胁安全攸关领域的基础设施，造成巨大的生命财产损失，所以配电物联网固件的安全成为了配电物联网安全的第一大要素[4-5]。面对配电物联网设备数量的高速增长、固件自身规模和复杂性的不断攀升、固件类型的日益多样化、固件故障的持续增多，有效的固件故障检测及预警是保障物联网设备安全的关键[6-7]。

配电物联网网络预警的关键在于配电物联网固件的故障检测。对此，王安娜等[7]提出一种基于感知-竞争混合神经网络的故障诊断方法，通过结合感知神经网络（BP，back propagation neural network）和竞争神经网络（ART, adaptive resonance theory）来识别分类多种故障，并通过改进传统的ART神经网络竞争机制，有效地对故障进行诊断。采用聚类方法进行故障诊断，能够降低故障类别维数，有利于故障的分类识别。李学军等[8]提出一种基于类均值核主元分析法的故障诊断算法，该算法通过将输入空间的数据样本映射到高维特征空间，求得类均值矢量，再通过子空间对类均值矢量进行主元分析，实现无信息损失的数据降维，对故障情况进行准确识别。曹源等[9]提出一种安全计算机状态监测方法，以视情维修为切入点，采用隐马尔可夫模型（HMM, hidden markov model）为研究工具，通过正常态模型训练与改进来实现安全计算机健康状态的检测，通过贝叶斯网络的概率推理准确定位根故障。周真等[10]提出了一种故障诊断中不确定性信息处理的贝叶斯网络方法，构建了一种基于事故树分析方法的3层贝叶斯网络模型，并通过模型进行故障推理。

对配电物联网固件进行检测后，采用故障自修复机制，查找出节点故障类型，并采取有效的能量分配方法来修复节点。在配电物联网固件自我恢复方面，蒋勇等[11]提出一种多属性加权模糊贝叶斯的复杂网络故障自修复机制。建立贝叶斯网络结构模型，针对故障节点进行条件概率估计，实现故障类别诊断。杨丽君等[12]提出一种基于动态联盟的配电网故障恢复策略。李学平等[13]基于多代理系统建立含分布式发电的配电网多故障抢修模型，考虑突发新故障后，通信正常和不正常2种情况的动态更新策略。黄弦超等[14]提出配电网多故障抢修与恢复的联合优化模型，应用快速非支配遗传算法进行恢复重构，但对顺序优化问题的求解模型较为简单。

综上所述，配电物联网网络预警与自愈技术研究重点就在于对配电物联网固件的故障检测与自我恢复的研究。文中提出适用于配电物联网边缘网络固件的安全防御技术框架，形成了具备安全预警及自愈能力的配电边缘物联网技术方案，并基于模拟实验验证了文中方案的可行性。

1 基础知识及系统模型

1.1 双线性映射

对2个乘法循环群 G_1 和 G_2，他们的生成元分别为 g 和 h，对于任何的 $p\in G_1$ 和 $q\in G_2$，双线性映射是一个映射 $e:G_1\times G_2\rightarrow G_T$，它具有以下性质。

1）双线性：选定任意的数字 $a, b\in Z$，满足 $e(p^a,q^b)=e(p, q)^{ab}$。

2）非退化性：映射不会把所有的元素对映射到 G_T 中的单位元，即 $e(g,h)\neq 1$。

3）可计算性：一定存在一个有效算法计算 $e(p,q)$。

1.2 密钥协商

Diff-Hellman算法是一种建立密钥的方法[15]，而不是加密方法，所以密钥必须和其他加密算法[16]结合使用。

用户 m 和用户 n 商定一个素数 q 和它的原根 g，之后每个用户随机选择一个与 q 互为质数的大整数作为私钥 X_n 和 X_m，并计算出 $Y_n=(g^{X_n} \bmod q)$ 和 $Y_m=(g^{X_m} \bmod q)$ 作为其公钥。通过共享公钥，可以生成用户 n 和用户 m 之间的交互密钥：

$$\mathrm{DH.gen}(X_n,Y_m)\rightarrow k_{n,m}=(Y_m)^{X_n} \bmod q=(g^{X_m} \bmod q)^{X_n} \bmod q=g^{X_nX_m} \bmod q, \tag{1}$$

$$\mathrm{DH.gen}(X_m,Y_n)\rightarrow k_{m,n}=(Y_n)^{X_m} \bmod q=(g^{X_n} \bmod q)^{X_m} \bmod q=g^{X_mX_n} \bmod q。 \tag{2}$$

很显然，$k_{n,m}=k_{m,n}=k$，因此可以用 k 作为对称加密算法[16]的密钥，比如加密：

$$\mathrm{AES.enc}(k,\mathrm{msg})\rightarrow \widehat{\mathrm{msg}}, \tag{3}$$

和解密：

$$\mathrm{AES.dec}(k,\widehat{\mathrm{msg}})\rightarrow \mathrm{msg}。 \tag{4}$$

1.3　秘密共享

秘密共享技术是密码学和信息安全的一个重要研究内容。Shamir秘密共享算法[17]基于拉格朗日插值法，其基本思想是分发者通过秘密多项式，将秘密 s 分解为 U 个分享值，任意大于等于 t 个的部分都可以重构，同时任意 t-1 个参与者无法获得秘密的任何信息。

约定一个大素数 q 和小于 q 的 t-1 个随机数 $\{a_1,a_2,a_3...a_{t-1}\}$，根据多项式

$$s_n=(s+a_1*n+...+a_{t-1}*n^{t-1}) \bmod q, \tag{5}$$

分别将各用户的编号 n 带入多项式，可以生成 n 个分享值：

$$\mathrm{SS.share}(u,t,s)\rightarrow\{(n,s_n)\}_{n\in U}, \tag{6}$$

其中，任意大于等于 t 个分享值的集合 $u_1\in u$，$u_1>t$ 都可以恢复原来的秘密：

$$\mathrm{SS.recov}(\{(m,s_m)\}_{m\in u_1},t)\rightarrow s。 \tag{7}$$

1.4　系统模型

配电物联网的架构是一种多点管理的架构，如图 1 所示，本架构主要考虑 3 部分实体：边缘服务器、边缘设备组和可信第三方。

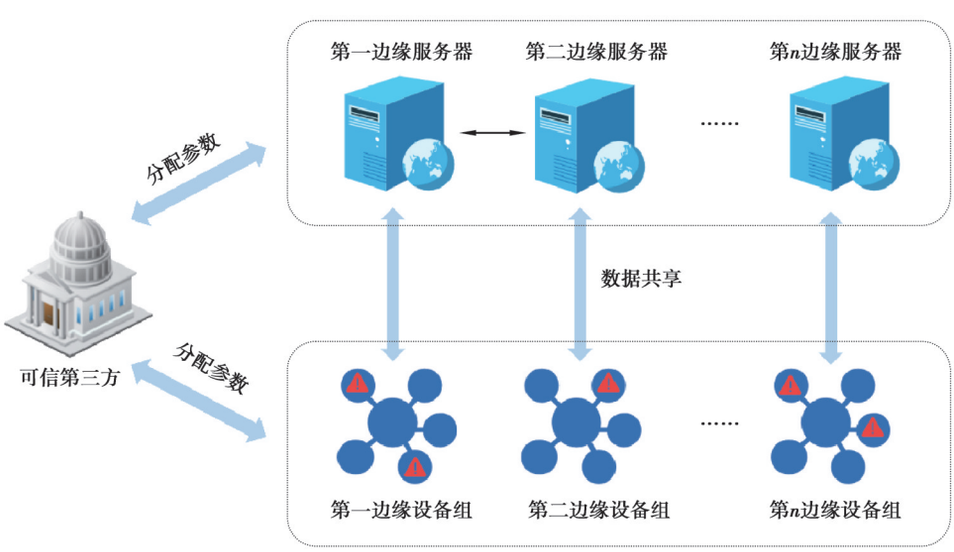

图 1　技术架构图

Fig. 1　Technical architecture diagram

每个区域的电网由一个边缘服务器负责管理，边缘服务器负责对该区域电网中的各边缘设备进行管理，称为边缘设备组。每个边缘服务器负责管理本区域的一组边缘设备，边缘设备中存有各个固件的可靠性矩阵，各边缘服务器相互连接，能够实现数据交互。

为了提高电网固件数据的安全性，各固件数据是存储在边缘设备本地的，并不向外发送实际的固件数

据。考虑到固件可能发生故障，设备易遭受恶意病毒攻击，且攻击者会通过非敏感信息，构造推断攻击模型去推断敏感信息，所以边缘设备需要对本地的固件运行情况进行检测，包括漏洞和恶意病毒检测，再对数据进行处理，将数据处理结果上传给边缘服务器。

2 详细方案

针对配电物联终端的固件故障检测问题，文中提出了基于联邦学习的架构，在实现检测功能的同时对各设备本地的固件隐私数据进行保护。

首先进行初始化，为后续的密钥交换和验证值计算初始化密钥对和随机数，提供给后续步骤使用，最终实现故障检测和隐私保护功能。在图 2 中，可信第三方服务器为第一边缘设备组的每个边缘设备初始化密钥对并选择多组随机数$(a_2,b_2),(a_3,b_3),\cdots,(a_n,b_n)$用于伪随机数生成器。然后，可信第三方服务器分别将每组随机数发送给各边缘服务器，例如将随机数(a_2,b_2)发送给第二边缘服务器，将随机数(a_3,b_3)发送给第三边缘服务器，以此类推。

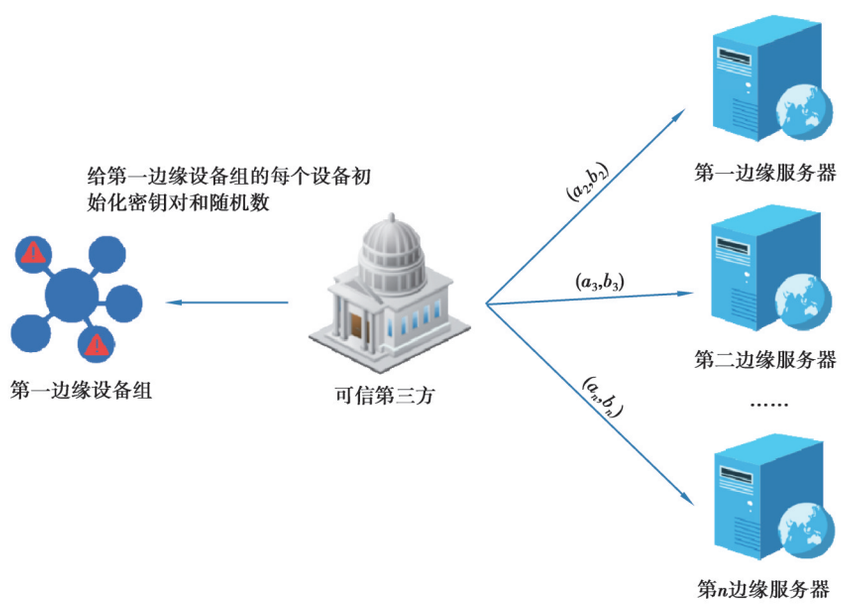

图 2 可信第三方初始化流程图

Fig. 2 Flow chart of trusted third party initialization

最后是密钥分享流程。初始化结束后的每个边缘设备都持有各自唯一的密钥对，该步骤将各设备的一些公开信息发送给服务器进行广播，以满足后续步骤需要。如图 3 所示，每个边缘设备组与边缘服务器之间进行密钥分享。

密钥分享完成后，各服务器和边缘设备组进行本地训练。为了提高电网固件数据的安全性，各固件数据是存储在边缘设备本地的，并不向外发送实际的固件数据。所以边缘设备需要对本地的固件运行情况进行检测，包括漏洞检测，再对数据进行本地的训练，将训练结果处理后上传给边缘服务器。

训练过程如图 4 所示。在第一边缘设备组中的边缘设备接收到固件可靠性矩阵后，根据公式$\boldsymbol{x}_u^*=(\boldsymbol{Y}\boldsymbol{C}^u\boldsymbol{Y}^{\mathrm{T}}+\lambda\boldsymbol{I})^{-1}\boldsymbol{Y}\boldsymbol{C}^u p(u)$计算出边缘设备矩阵的更新值$\boldsymbol{x}_u^*$，其中，矩阵$\boldsymbol{Y}$是存储于第一边缘服务器的固件可靠性矩阵，$p(u)$代表固件是否可靠，矩阵$\boldsymbol{C}$代表固件的可靠性程度，然后根据公式$\boldsymbol{x}_{ui}^n=[c_{ui}(p_{ui}-\boldsymbol{x}_u^{\mathrm{T}}\boldsymbol{y}_i)]\boldsymbol{x}_u$计算出本地梯度向量$\boldsymbol{x}_{ui}^n$，其中，$c_{ui}$和$p_{ui}$为第$u$个边缘设备中存储的第$i$个元件的可靠性数据，$p_{ui}$代表固件是否可靠，$c_{ui}$代表固件的可靠性程度，$\boldsymbol{y}_i$代表第$i$个元件的可靠性。接着将本地梯度向量进行双重加密，生成加密的本地梯度向量$\widehat{\boldsymbol{x}_{ui}^n}$，$\widehat{\boldsymbol{x}_{ui}^n}=\boldsymbol{x}_{ui}^n+P_{\mathrm{RG}}(\beta_n)+\sum_{m\in u_2,m>n}P_{\mathrm{RG}}(k_{n,m})-\sum_{m\in u_2,m<n}P_{\mathrm{RG}}(k_{n,m})$，其中，$P_{\mathrm{RG}}(m)$是一种以 m

为种子的伪随机数生成器,U_2为密钥共享阶段边缘设备列表。

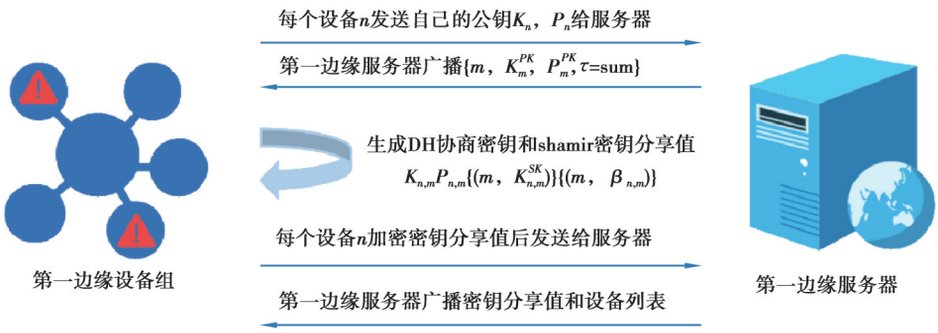

图 3　密钥分享流程图

Fig. 3　Key sharing flowchart

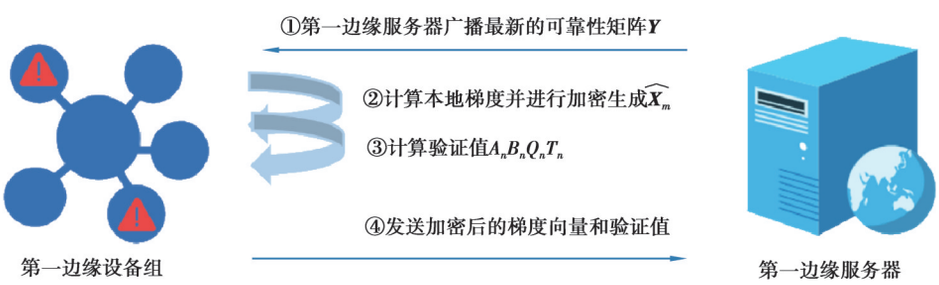

图 4　本地训练流程图

Fig. 4　Local training flow chart

目前对于物联网攻击程序的甄别主要是通过对比控制流图和已知的恶意攻击的相似度进行判断。然而该办法并不能有效地阻止精心设计的变种攻击。因此,文中提出验证方法,用于对恶意数据的检测。第一边缘设备组中的边缘设备根据如下公式计算验证所需参数 U_n、I_n、Q_n、T_n:

$$\mathrm{HE}(x_1^n)=(U_n,I_n)=(g^{\mathrm{HF}_{\delta,\rho}(x_1^n)},h^{\mathrm{HF}_{\delta,\rho}(x_1^n)}),\tag{8}$$

$$\mathrm{PF}_{a_2,b_2}(n,\tau)=(R_n,S_n)=(g^{a_{2n}a_{2\tau}+b_{2n}b_{2\tau}},h^{a_{2n}a_{2\tau}+b_{2n}b_{2\tau}}),\tag{9}$$

$$Q_n=(R_nU_n^{-1})^{1/d}=(g^{a_{2n}a_{2\tau}+b_{2n}b_{2\tau}-\mathrm{HF}_{\delta,\rho}(x_1^n)})^{1/d},\tag{10}$$

$$T_n=(S_nI_n^{-1})^{1/d}=(h^{a_{2n}a_{2\tau}+b_{2n}b_{2\tau}-\mathrm{HF}_{\delta,\rho}(x_1^n)})^{1/d}。\tag{11}$$

式中:HE()是一种同态哈希函数;$\mathrm{HF}_{\delta,\rho}()$是以$\delta$、$\rho$为生成密钥的抗碰撞的同态加密函数;$\mathrm{PF}_{a,b}()$是以$a$、$b$为种子的伪随机数生成器;$g$和$h$分别是群$G_1$和$G_2$的生成元。

所有服务器发送完毕后,进行联合训练及检测。边缘服务器将管理的各边缘设备上传的数据聚合后,安全地共享给其他边缘服务器,并结合其他边缘服务器共享的数据来更新各固件的可靠性。同时,检测针对物联网设备恶意攻击是巩固物联网系统不可或缺的环节。各服务器会根据上一步发送的数据进行数据验证,以保证训练结果的真实性。

边缘服务器间联合训练及检测流程如图 5 所示。

第一边缘服务器重组密钥,并完成梯度聚合,生成聚合梯度:

$$\Theta_1=\sum_{n\in u_3}\widehat{x_{ui}^n}-\sum_{n\in u_3}\mathrm{PRG}(\beta_n)-\sum_{n\in(u_2-u_3),m\in u_3,m>n}\mathrm{PRG}(k_{n,m})+\sum_{n\in(u_2-u_3),m\in u_3,m<n}\mathrm{PRG}(k_{n,m})。$$

第一边缘服务器和第一边缘设备组中的各服务器之间可以根据图 4 所示本地训练流程图完成梯度聚合。同时,第一边缘服务器计算验证:

$$\{U,I,Q,T\}\leftarrow U=\prod_{n=1}^{n=|u_3|}U_n,I=\prod_{n=1}^{n=|u_3|}I_n,Q=\prod_{n=1}^{n=|u_3|}Q_n,T=\prod_{n=1}^{n=|u_3|}T_n。\tag{12}$$

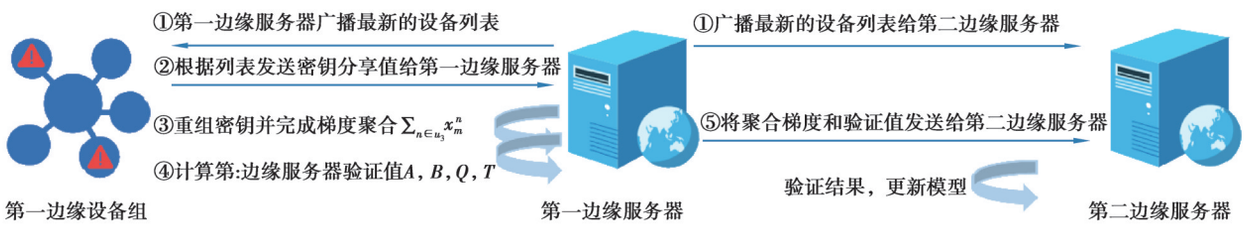

图 5 边缘服务器间联合训练及检测流程图

Fig. 5 Flowchart of joint training and detection among edge servers

其他边缘服务器根据本地随机数和第一边缘设备组成员列表验证第一边缘服务器发送的聚合结果，如果满足

$$e(U,h)\,e(Q,h)^{d}=e(g,h)^{\sum_{n\in u_3}(a_{2n}a_{2\tau}+b_{2n}b_{2\tau})},e(U,h)=e(g,I),e(Q,h)=e(g,T),\tag{13}$$

$$(U,I)=(U',I')=(g^{\mathrm{HF}_{\delta,\varphi}(\sum_{n\in u_3}x_1^n)},h^{\mathrm{HF}_{\delta,\varphi}(\sum_{n\in u_3}x_1^n)}),\tag{14}$$

则其他边缘服务器认可第一边缘服务器发送的数据的真实性，并以此更新固件可靠性矩阵。式(13)中，$e()$为双线性映射方法。

通过上述提出的基于人工智能和联邦学习的算法可对固件的可靠性进行有效评估，从而实现对固件漏洞进行检测与修复。

确定了固件的故障情况后，文中提出自适应的固件自我恢复方法。在网络总体能量有限的情况下，适当地分配给故障设备一部分能量，使其能够重新工作。对于能量的分配方法，需要结合可分配能量情况、各设备的平均能量情况，以及故障设备的能量衰减情况、故障设备数。

假设网络中可分配的能量总量为$E(X)$，故障设备数量为k，故障设备集为T，总设备数量为n，对于$E(x_i)$剩余能量为故障设备x_i所需要补充的能量为

$$E(x_i)=E_T-E(x_i)+\sum_{j=1}^{n}E(x_j)/n。\tag{15}$$

同时，对于区域互联形成的子区域，每个边缘设备组将需要抢修的故障固件信息传递给边缘服务器，边缘服务器控制能源调度系统对附近的抢修小队进行调度，以减少抢修时间，提高修复效率。如果抢修2个故障恢复的失电负荷相同，则可以先抢修故障修复时间短的故障，待所有失电负荷全部恢复供电之后，再抢修另一故障固件。

3 安全分析与性能实验

3.1 安全分析

文中算法的安全性分析基于“诚实但好奇”的模型。在此模型中，可信第三方是完全可信的，可以将初始化的任务交付给可信第三方执行，以保证后续所有步骤的真实可靠。

所有边缘服务器和边缘设备都被认为是诚实但好奇的，也就是说，边缘服务器和边缘设备都按照约定协议执行程序，边缘设备会如实地检测各固件的运行情况，并按照协议要求对固件隐私数据进行处理和上传，各边缘服务器如实按照协议要求对固件可靠性数据进行聚合和分享，以完成整个固件故障检测的流程。但同时，他们也可以尝试独立推断其他参与者的数据隐私，例如窥探某一个边缘设备的固件故障以及可靠性的隐私数据。此外，对于一个参与者，允许少于t的设备或边缘服务器之间的任何合谋，这意味着边缘服务器可以与多个边缘设备中的设备勾结，以获得最大的攻击能力。

首先，单个边缘设备只能从边缘服务器中获得最新的固件可靠性矩阵，这不涉及其他边缘设备上数据，也就不会带来安全问题。对边缘服务器来说，在全局训练的过程中，每个边缘设备对自己上传的本地梯度进行了加密，边缘服务器无法获知任何一个梯度的原始值，进而无法由此推断出某个边缘设备的固件隐私

信息。

其次,在边缘服务器间联合训练流程中的密钥恢复阶段,边缘服务器只能恢复所有在线边缘设备和所有掉线边缘设备的密钥,这不足以对梯度进行解密。对于合谋攻击,由于Shamir秘密共享方案的阈值设置,任何小于t个边缘设备的共享值都无法重构秘密,也就无法得到比边缘服务器更多的信息。

再次,通过固件可靠性矩阵,可以对物联网固件设备进行检测和修复,判断其是否可信。并采用人工智能技术对问题固件进行快速修复,保证系统安全运行。

最后,针对配电物联网中的恶意病毒攻击,设计基于深度学习模型和人工智能技术的自进化物联网恶意程序检测及防御模型,实现对物联网恶意病毒的实时快速检测与防御。

综上所述,在文中的威胁模型下,边缘设备上数据得到了有效的保护,能有效实现对物联网固件恶意漏洞和恶意病毒的快速检测与修复。

3.2　性能实验

实验的主要任务是测试该方案在不同设置下的对设备的计算消耗。实验模拟了3个边缘服务器,并将边缘设备平均分配到每个边缘服务器。不失一般性,文中实验只展示了第一边缘服务器的性能。

为了减少随机性对实验的影响,将每个实验重复10次,取其平均值。一般来说,运行时间由5个部分组成:初始化、边缘设备更新、设备自愈恢复、服务器更新和验证,其中实验用一个迭代中所有边缘设备更新成本的平均值来代表边缘设备更新时间,用一个边缘服务器在所有迭代中的平均时间来代表边缘服务器更新时间。

首先,实验评估了不同固件数量的影响。为了消除其他变量的影响,实验将边缘设备数设定为50。图6显示了不同固件数下的运行时间。相比之下,边缘设备更新、设备自愈恢复和验证3部分的时间比较少,无法在图中清晰显示,所以在图7中分别画出了这3个数值。如图所示,实验可以推断出,随着固件数量的增加,边缘服务器更新时间呈线性增加,而其余4项基本保持稳定。

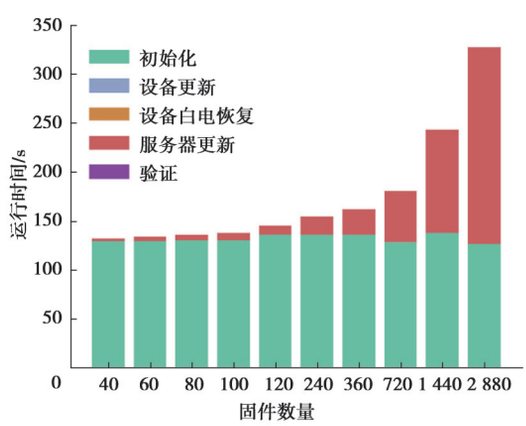

图6　不同固件数量的运行时间(1)

Fig. 6　Runtime for different quantities of firmware(1)

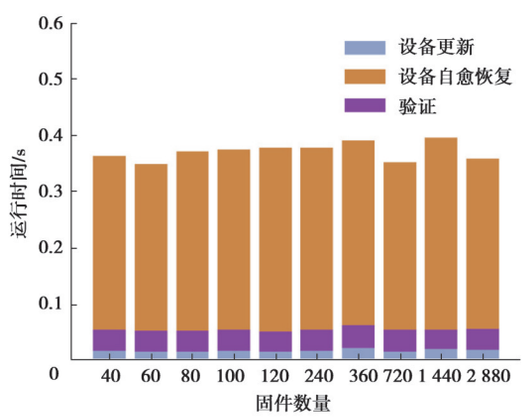

图7　不同固件数量的运行时间(2)

Fig. 7　Runtime for different quantities of firmware(2)

然后,本实验用均方根误差(RMSE,root mean square error)来评估系统的性能。如图8所示,随着固件数量的增加,系统的RMSE在120个轮次后保持在1.0左右,这表明固件数量几乎不影响RMSE。

本实验进一步评估了不同边缘设备数量的影响。将固件的数量设置为240个。图9显示了不同边缘设备数下的运行时间。为了使数据更加直观,在图10中画出了边缘设备更新和验证时间,在图11中画出了设备自愈恢复和边缘服务器更新时间。很明显,边缘设备数基本上不影响边缘设备更新时间和验证时间。随着边缘设备数量的增加,初始化所需的时间受影响最大,并呈指数级增长。然而,如前所述,如果没有边缘设备退出,系统初始化只需执行一次。边缘设备数量的增加也会影响边缘服务器的更新时间和重组时间。随

着边缘设备数量的增加,这 2 个时间呈线性增长。

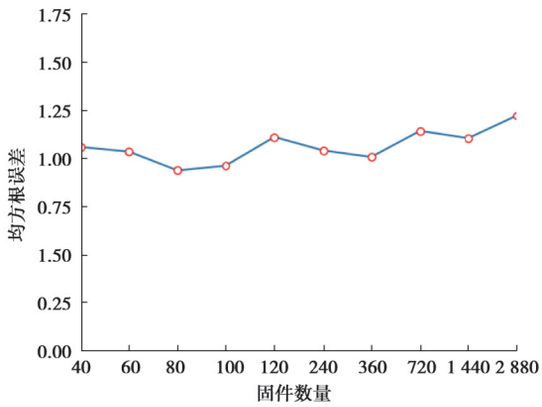

图 8 不同固件数量的 RMSE

Fig. 8 RMSE for different quantities of firmware

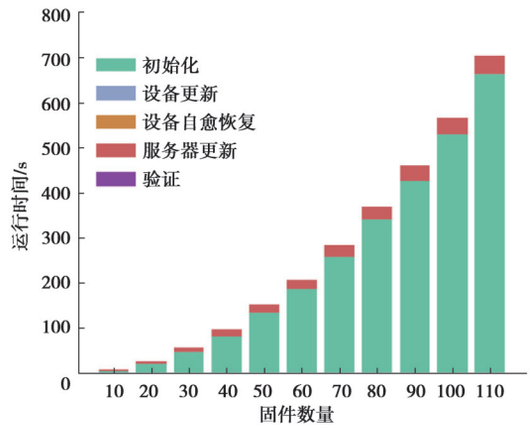

图 9 不同边缘设备的运行时间(1)

Fig. 9 Runtime for different edge devices(1)

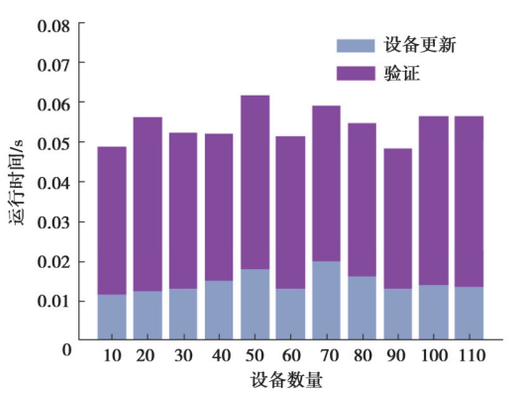

图 10 不同边缘设备的运行时间(2)

Fig. 10 Runtime for different edge devices(2)

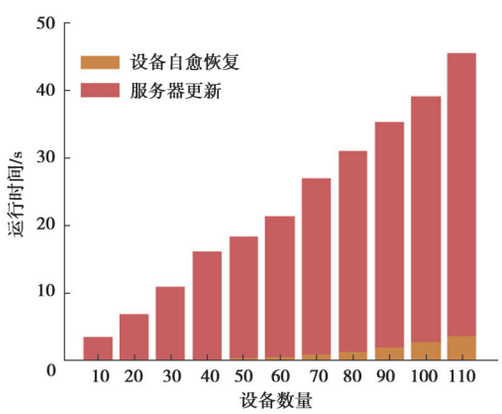

图 11 不同边缘设备的运行时间(3)

Fig. 11 Runtime for different edge devices(3)

最后,实验评估了不同数量的故障边缘设备的影响。由于边缘设备数量和固件数量是恒定的,实验主要观察了设备自愈恢复时间的影响。如图 12 所示,随着故障边缘设备数量的增加,设备自愈恢复所花费的时间也在线性增加,这与实验对系统的设想一致。

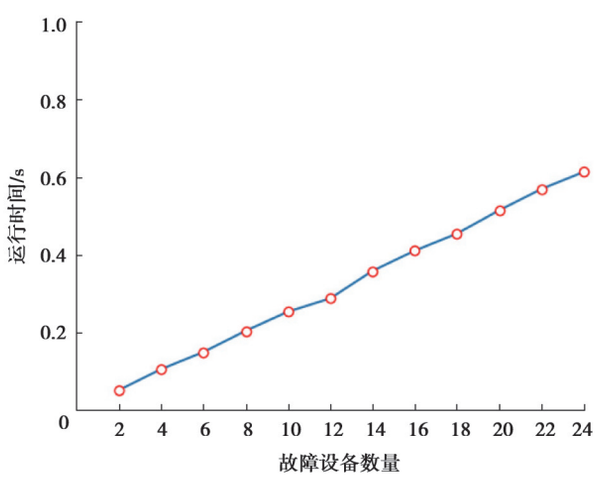

图 12 不同故障边缘设备的恢复时间

Fig. 12 Recovery time for different failed edge devices

4　结束语

由于配电物联网的运行大量依赖于其固件,配电物联网网络预警与自愈技术的研究重点在于配电物联网固件的故障检测与自我恢复,因此提出了一个适用于配电物联网边缘网络固件的安全防御技术框架,形成了具备安全预警及自愈能力的配电边缘物联网技术方案。文中方案基于联邦学习,允许多个边缘服务器参与联合建模。每个边缘服务器的边缘设备组在本地用自己的数据参与训练,在不泄露单个边缘设备隐私数据的前提下,生成固件可靠性矩阵,通过联邦架构安全地交换中间数据,实现对固件漏洞及设备的快速检测已经自适应地恢复。讨论了该方案的安全性,并基于真实数据集进行相关实验,验证了所提出方案的高效性和可行性。

参考文献

[1] 冯杨. 电网数字化转型下面临的安全形式与保障措施研究[J]. 通信电源技术, 2021, 38(3): 206-208.
Feng Y. Research on security forms and safeguard measures in the digital transformation of power grid[J]. Telecom Power Technology, 2021, 38(3): 206-208.(in Chinese)

[2] 王琨, 杜亮, 马来·对山拜, 等. 面向智能电网应用的电力大数据关键技术研究[J]. 微型电脑应用, 2021, 37(8): 123-126.
Wang K, Du L, Ma L, et al. Research on key technologies of power big data for smart grid application[J]. Microcomputer Applications, 2021, 37(8): 123-126.(in Chinese)

[3] Wang Q P, Group X, Bo Z Q, et al. Integrated wide area protection and control for power grid security[J]. CSEE Journal of Power and Energy Systems, 2019, 5(2): 206-214.

[4] Guo Q, Zhu Y H, Chang D X, et al. A remote test method for power grid security and stability control system and its engineering application[J]. E3S Web of Conferences, 2021, 260: 02006.

[5] 王瑾, 裴亮. 基于深度学习的电网调控系统异常检测与多阶段风险预警[J]. 沈阳工业大学学报, 2021, 43(6): 601-607.
Wang J, Pei L. Anomaly detection and multi-stage risk pre-warning technology of power grid control system based on deep learning [J]. Journal of Shenyang University of Technology, 2021, 43(6): 601-607. (in Chinese)

[6] Zhang S, Luo X C, Litvinov E. Serverless computing for cloud-based power grid emergency generation dispatch[J]. International Journal of Electrical Power & Energy Systems, 2021, 124: 106366.

[7] 王安娜, 刘坐乾, 杨铭如, 等. 基于BP-ART混合神经网络的电路故障诊断新方法[J]. 系统工程与电子技术, 2010, 32(4): 873-876.
Wang A N, Liu Z Q, Yang M R, et al. Novel method for circuit fault diagnosis based on the BP-ART hybrid neural network[J]. Systems Engineering and Electronics, 2010, 32(4): 873-876.(in Chinese)

[8] 李学军, 李平, 蒋玲莉. 类均值核主元分析法及在故障诊断中的应用[J]. 机械工程学报, 2014, 50(3): 123-129.
Li X J, Li P, Jiang L L. Class mean kernel principal component analysis and its application in fault diagnosis[J]. Journal of Mechanical Engineering, 2014, 50(3): 123-129.(in Chinese)

[9] 曹源, 马连川, 李旺. 铁道信号系统安全计算机状态监测方法[J]. 交通运输工程学报, 2013, 13(3): 107-112.
Cao Y, Ma L C, Li W. Monitoring method of safety computer condition for railway signal system[J]. Journal of Traffic and Transportation Engineering, 2013, 13(3): 107-112.(in Chinese)

[10] 周真, 周浩, 马德仲, 等. 风电机组故障诊断中不确定性信息处理的贝叶斯网络方法[J]. 哈尔滨理工大学学报, 2014, 19(1): 64-68.
Zhou Z, Zhou H, Ma D Z, et al. Method of Bayesian network for uncertainty information processing of wind turbines fault diagnosis[J]. Journal of Harbin University of Science and Technology, 2014, 19(1): 64-68.(in Chinese)

[11] 蒋勇, 赵作鹏. 多属性加权模糊贝叶斯的复杂网络故障自修复技术[J]. 计算机应用研究, 2015, 32(8): 2378-2381.
Jiang Y, Zhao Z P. Complex network fault self-repair mechanism with multi-attribute weighted fuzzy Bayesian[J]. Application Research of Computers, 2015, 32(8): 2378-2381.(in Chinese)

[12] 杨丽君, 于琦, 魏玲玲, 等. 基于移动多代理动态联盟的配电网故障恢复研究[J]. 电工技术学报, 2016, 31(8): 147-155.
Yang L J, Yu Q, Wei L L, et al. A distribution network fault recovery study on the dynamic alliance of mobile multi-agent[J]. Transactions of China Electrotechnical Society, 2016, 31(8): 147-155.(in Chinese)

[13] 李学平, 卢志刚, 刘照拯, 等. 含分布式电源的配电网多故障抢修的多代理策略研究[J]. 电工技术学报, 2013, 28(8): 48-55.
Li X P, Lu Z G, Liu Z Z, et al. Multi-agent strategy of distribution networks multi-faults rush-repair with distributed generators [J]. Transactions of China Electrotechnical Society, 2013, 28(8): 48-55.(in Chinese)

[14] 黄弦超, 杨雨,范闻博. 配电网故障抢修与供电恢复联合优化模型[J]. 电力系统自动化, 2014, 38(11):68-73.
Huang X C, Yang Y, Fan W B. Combined optimization model for maintenance scheduling and service restoration of distribution system[J]. Automation of Electric Power Systems, 2014, 38(11):68-73. (in Chinese)

[15] Diffie W, Hellman M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[16] Kaur G, Madaan N. A comparative study of AES encryption decryption[J]. Journal of Innovation and Social Science Research, 2015, 2(6): 84-88.

[17] Shamir A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

（编辑　詹燕平）