

无线通信网络非信任内网区域 与信任区域的网络安全连接方法

庄君丰[†], 郑挺

(浙江省公安科技研究所, 浙江 杭州 310000)

摘 要:在无线通信网络中,数据交互通过多组信息节点的发送请求、确认身份、接收认证信息过程,实现不同区域消息的交换与连接。非信任内网区域与信任区域之间的连接与一般区域连接不同,受到信任值差异的影响,在连接过程中容易受到扰动节点信息影响,连接成功率大幅度降低;甚至在局部节点信号噪声扰动下,无法保证节点数据连接安全,致使无线通信网络全局信息使用存在被攻击风险。为了解决非信任内网区域与信任区域的网络安全连接问题,通过无线通信网络非信任内网区域与信任区域博弈模型构建、无线网络信任区域信任值计算、非信任内网区域信任值计算以及无线通信网络非信任内网区域与信任区域的网络安全连接,对其连接节点及其区域参量进行博弈评价,并根据模型对其区域信任值进行优化,进而实现安全连接的效果。通过实验数据进一步证明了提出方法的有效性与可行性。

关键词:无线通信网络;非信任内网区域;信任区域;安全连接

中图分类号:TM773

文献标识码:A

Network Secure Connection Method of Non-trusted Intranet Area and Trusted Area of Wireless Communication Network

ZHUANG Junfeng[†], ZHENG Ting

(Zhejiang Public Security Institute of Science and Technology, Hangzhou, Zhejiang 310000, China)

Abstract:In the wireless communication network, data interaction realizes the exchange and connection of messages in different regions through the process of sending the request of multiple groups of information nodes, confirming identity and receiving authentication information. In this process, the connection between the non-trusted Intranet area and the trusted area is different from the general area connection, and the connection success rate is greatly reduced. Under the signal noise disturbance of local nodes, the security of node data connection cannot be guaranteed, resulting in the risk of attacking the global information use of wireless communication network. In order to solve the problem of network security connection between non-trusted intranet area and trust area, the game model construction of non-trusted internal network area and trust area, the calculation of trust value of wireless network, and the network security connection between the non-trusted intranet area and trust area of wireless communication network shall evaluate the connection nodes and the regional trust value according to the model to realize the effect of secure connection. The effectiveness and feasibility of the proposed method are further proved by the experimental data.

Key words:wireless communication network; non-trusted Intranet area; trusted area; secure connection

无线网络中内网非信任区域与外网信任区域接入点(AP)之间通过无线网络进行数据传输,因此对这两个区域的安全防护是十分重要的。目前,在无线网络中使用的信任安全连接方法主要包括 TLS、IDLE、WPA/WPA2 等^[1-2],其中,TLS 是最常用的一种。众多学者针对网络信息安全问题进行了大量研究,如文献[3]收集无线网络数据安全数据,使用 Apriori 算法深度挖掘无线网络数据安全关联数据,搭建网络安全态势感知模型,基于深度学习实现无线网络数据安全态势感知。文献[4]分析网络信息安全现状,把网络与信息的安全防护放在重要位置,以内网信息安全需求为落脚点,构建信息安全防护系统。但是在实际应用中,由于 TLS 安全连接节点会在传输数据过程中造成两区域消息交换的较大时延^[5],所以不能很好地满足用户需求。为此,如何解决无线网络下非信任内网区域与信任区域连接及其连接安全问题,成为众多研究人员与学者的讨论重心。

1 连接方法的具体实现

1.1 无线网络非信任内网区域与信任区域博弈模型构建

考虑到无线网络非信任内网区域与信任区域之间连接节点认证具有博弈性,因此在信任区域与非信任区域连接过程中,两区域交界处相邻节点之间需要相互获取信息,基于自组织网络结构属性特征,对其信息特征进行博弈模型构建,构建过程中对其相关参量作如下假设。

1)全局无线网络区域(包括信任区域与非信任区域)由 N 个逻辑配置节点构成,信任区域与非信任区域交互过程构成间接信任交互过程,即连接节点会向其对应的相邻节点发送其所在区域的部分信息,以此作为连接请求,在这个过程中不包含其他形式信息或报文的转发。

2)在连接过程中对应网络空间的时间具有统一性,其时间系数由一系列离散时隙 t 确定,其中,每一个对应时隙对应一个小博弈空间^[6],受其影响每个节点至少会向相邻节点发送一个间接信任请求信息,且不会影响当前网络状态,保证不同层级链路节点的正常通信。

3)在博弈空间下,任意节点连接相邻节点完成

间接信任交互过程所消耗的能量均相同^[7-8],其能量系数为 c ,考虑到回传消息由认证机制决定,因此在博弈模型中不考虑节点回传消息所消耗的能量。

基于上述假设,无线网络非信任内网区域与信任区域的间接信任连接博弈模型构建过程如下。

定义 1:间接信任连接过程中信任区域与非信任区域交界处相邻节点获取信息的基本关系函数为一个三元组^[9-10], $G = (P, S, \mu)$,其中, P 代表包含交界处相邻两个节点博弈特征的集合, $P = \{i, j\}, i, j \in N$, N 代表全局网络构成节点组成的集合, S 代表连接过程中任意一个节点自身能够获得信息集, $S = \{s_1, s_2\} = \{\text{信任区}(C), N\}$, μ 代表节点交互函数。

定义 2:一个节点 i 对应时隙为 t 时的交互函数具有博弈特征普遍性,则无线网络非信任内网区域与信任区域博弈模型为:

$$\mu_i(S_i^t, S_j^t) = S_j^t b_i - S_i^t (cn_i^t - p) \tag{1}$$

其中, S_i^t, S_j^t 分别代表节点 i 与节点 j 对应时隙为 t 时所匹配的博弈系数; b_i 代表当对应区域内相邻节点的博弈结果为合作时,节点 i 的增幅效果, $b_i = \delta e^{w^t}$,其中, δ 代表在相邻节点博弈结果为合作时,节点 i 能够获得的最大增幅系数, w^t 代表间接信任连接过程中节点 i 所获得增幅系数对应的信任因子, $0 \leq w^t \leq 1$; n_i^t 为节点 i 在一个时隙内发送间接信任请求信息的最大系数; p 代表节点 i 处于间接信任状态下的博弈损失。

与其效用相同,节点 j 对应博弈交互函数为:

$$\mu_j(S_i^t, S_j^t) = S_j^t b_i - S_i^t (cn_i^t + p) \tag{2}$$

若节点 i 博弈结果为合作,那么通过对应区域内节点的间接信任连接请求,此时 $S_i = 1$,否则节点将不做信息反馈, $S_i = 0$ 。构建模型内两个相邻节点建立间接信任时的博弈增幅矩阵如表 1 所示。

表 1 信任区域与非信任区域博弈增幅矩阵

博弈节点 (i, j)	j 合作 (C)	j 不合作 (U)
i 合作 (C)	$(b_i + cn_i^t - p, b_j - cn_j^t + p)$	$(-cn_i^t + p, b_j)$
i 不合作 (C)	$(b_i + cn_i^t - p)$	$(0, 0)$

1.2 无线网络信任区域信任值计算

基于上述信任区域与非信任区域的博弈模型,对无线网络信任区域信任值进行计算。从博弈模型节点间接信任连接结果入手,分别定义相邻节点间接信任连接博弈结果为合作时的信任评估为 $S_{i,j}$,不合作时的信任评估为 $F_{i,j}$ 。例如,若节点 i 与相邻节点 j 之间的直接信任值为 $0.7^{[11-12]}$,则可认为下一周期节点 j 对应的直接信任值无限趋近于 0.7 ,甚至等于 0.7 。若下周期节点 j 对应的直接信任值大于或等于 $(0.7 - \sigma)$,则认为此状态下节点信任评估指标有效。若下周期节点 j 对应信任值小于 $(0.7 - \sigma)$,则认为此状态下节点信任评估指标无效。计算过程中令 $\sigma = DT_{i,j}(t) \times 100\%$ 。则信任区域连接控制因子 f 的函数关系式可以描述为:

$$f = \frac{S_{i,j} + 1}{S_{i,j} + F_{i,j} + 1} \quad (3)$$

将信任区域连接控制因子 f 与信任值 $DT_{i,j}(t)$ 进行乘积运算,可获得不同区域下两个节点连接时信任值的控制系数,若所得系数值对其他节点 k 正常通信造成的影响较小, n 代表节点集合 C_n 所包含的元素总量,则对信任值 $DT_{i,j}(t)$ 计算公式作如下更新:

$$DT_{i,j}(t) = \frac{\sum_{k=1}^n b_k (S_{i,j} + 1)}{\sum_{k=1}^n b_k (S_{i,j} + F_{i,j} + 1)} \quad (4)$$

1.3 非信任内网区域信任值计算

完成信任区域的信任值计算后,相应地对非信任内网区域信任值展开计算。根据博弈模型中其它节点对节点 j 的博弈反馈效果,首先对其博弈反馈效果进行二次甄别^[13],然后对筛选结果进行权重分配,最后得到非信任内网区域信任值 $IT_{i,j}(t)$ 。

非信任内网区域信任值的原始计算公式为:

$$IT_{i,j}(t) = \sum_{k \in C_f} w_k \times RT_{i,j}^k(t) \quad (5)$$

式中: C_f 代表筛选后剩余节点组成的合集。 w_k 代表具有相同属性特征的相邻节点 k 所对应权重系数, $RT_{i,j}^k(t)$ 代表相邻节点 k 对节点 j 的信任值系数,根据计算模型情况,取值为 $10^{[14]}$ 。

在计算非信任内网区域信任值 $IT_{i,j}(t)$ 时,考虑到该区域部分节点的信任系数存在偏差,因此在采用过程中需要对其偏差进行修正。其修正过程

将某个具有相同属性特征的邻节点 k 进行节点 j 的信任值 $RT_{i,j}^k(t)$ 映射,可得到:

$$RT_{i,j}^k(t) = DT_{i,k}(t) \times DT_{k,j}(t) \quad (6)$$

式中: $DT_{i,k}(t)$, $DT_{k,j}(t)$ 分别代表节点 i 对节点 k 的修正信任值与节点 k 对节点 j 的修正信任值。

映射信任值所对应的修正信任真实值 $RIT_{i,j}(t)$ 为:

$$RIT_{i,j}(t) = \frac{\sum_{k \in C_n} RT_{i,j}^k(t)}{n} \quad (7)$$

式中: C_n 代表节点 i 、 j 在该区域下的共同属性节点所构成的集合。

为了保证计算所得非信任内网区域信任值偏差在可控范围内,将非信任内网区域内具有共同属性特征的节点 l 进行偏离系数 d_l 约束:

$$d_l = \frac{1}{m-1} \sum_{l=1, l \neq k}^m \sqrt{[RT_{i,j}^k(t) - RT_{i,j}^l(t)]^2} \quad (8)$$

式中, d_l 对应系数值越大,对应节点 l 的信任值越小,反之, d_l 对应系数值越小,对应节点 l 的信任值越大, m 表示节点 l 的数量。

1.4 无线通信网络非信任内网区域与信任区域的网络安全连接

基于上述信任值,对无线通信网络非信任内网区域与信任区域进行网络安全连接。考虑到不同信任值下安全连接权重 CSI 是时变的,常规连接策略会受到信噪比偏差影响,因此将两区域安全连接过程视为用户 A 与 B 不同信任值下 P_A 和 P_B 安全连接权重 CSI 系数 ζ_1 和 ζ_2 的获取过程。

设各区域中不同节点的真实连接信任系数所对应信道为 $h_{ij} = \tilde{h}_{ij} + \Delta h_{ij}$,其中 $\tilde{h}_{ij}$ 代表信道 h_{ij} 的预测值, Δh_{ij} 代表信道连接过程中的预测偏差,且偏差值在信任值约束范围内,提出方法将其设为 $|\Delta h_{ij}| \leq \epsilon_{ij}$,其中 ϵ_{ij} 代表预测偏差值的最大系数,将其定义为偏差界。则两区域信息连接过程的第 2 阶段, B 根据信道预测值 $\tilde{h}_{ij}$ 将连接系数 $\tilde{y}_B$ 中的信噪比 S_B 和信噪比 S_J 进行滤除,得到滤波后两区域连接系数的关系数表达式:

$$y_B \approx \sqrt{(1 - \epsilon_{ij})} G(\sqrt{P_A \tilde{h}_{BR}} \tilde{h}_{AR} P_B + \tilde{h}_{BR} \zeta_1 + \Delta h_{BR} \zeta_2) + G(\tilde{h}_{BR} + \Delta h_{BR}) \quad (9)$$

式中, $\tilde{h}_{AR}$, $\tilde{h}_{BR}$ 与 $\tilde{h}_{JR}$ 分别代表 B 建立连接时所获取的 $A-R$, $B-R$ 与 $J-R$ 信道预测值,

Δh_{AR} , Δh_{BR} 与 Δh_{JR} 代表连接信道预测偏差。

结合实际连接情况下的成功率,无线网络非信任内网区域与信任区域的网络安全连接系数为 $h_{ij} = |\tilde{h}_{ij}| + |\Delta h_{ij}| = |\tilde{h}_{ij}| + \epsilon_{ij}$ [15], 则得无线网络非信任内网区域与信任区域的网络安全连接系数为:

$$\tilde{R}_S = \frac{1}{2} \left[\log_2 \left(\frac{(1 + \tilde{\gamma}_A)(1 + \tilde{\gamma}_B)}{1 + \tilde{\gamma}_B} \right) \right] \tag{10}$$

$\tilde{\gamma}_A$ 与 $\tilde{\gamma}_B$ 分别为信任区域与非信任区域连接过程中的信道安全指标,其对应系数为非零实数。

2 应用测试

对提出方法的安全连接性能进行测试。测试在仿真环境下完成,通过数据对比的方式得出结论。其中用于对比的参照方法选取 3 种不同连接方法,分别为基于博弈的无线网络安全连接方法,标记为参照方法 A;基于防御攻击特征的非信任区域无线网络安全连接方法,标记为参照方法 B;一种基于安全熵的无线网络连接方法,标记为参照方法 C;提出方法按照测试标准,标记为验证方法。在统一设定的环境与条件下,完成性能指标测试、统计、分析,得出最终结论。

2.1 仿真测试环境配置

考虑到当前网络环境数据的复杂性与多重性,为了保证测试数据样本具有客观性与代表性,测试样本采用随机样本;测试环境由 1 台内网服务器、3 台外网服务器构成数据平台,搭建测试平台网络结构如图 1 所示。

2.2 连接性能测试

在内网服务器中创建非信任区域,外网服务器均设置为信任区域,分别在两区域中随机 300 组数据作为测试样本包,其中包含信任区域连接请求数据样本 200 组与非信任区域连接请求数据 200 组;分别由参照方法 A、B、C 及验证方法对其进行连接调试,调试日志由仿真测试工具获取,提取连接指标数据后生成曲线图,如图 2 所示。

根据图 2 中不同方法测试曲线状态及其分布情况可知,参照方法 A 的连接稳定性波动最为剧烈,且变化频率值较小,无规律性,经过整理统计后得到参照方法 A 的均值连接成功率为 95.8%;参照方法 B 的连接效果较好,无较大波动,经过统计整理后得到其均值连接成功率为 97.4%;参照方

法 C 曲线波动幅度较大,且呈衰减趋势,经过统计得到其均值连接成功率为 92.8%;验证方法的曲线整体状态最好,无大幅度波动,无衰减现象出现,经过统计其均值连接成功率为 98.3%;由此得到不同方法在非信任内网区域与信任区域连接测试中,连接成功率按照由大到小的顺序排列为:验证方法-参照方法 B-参照方法 A-参照方法 C。

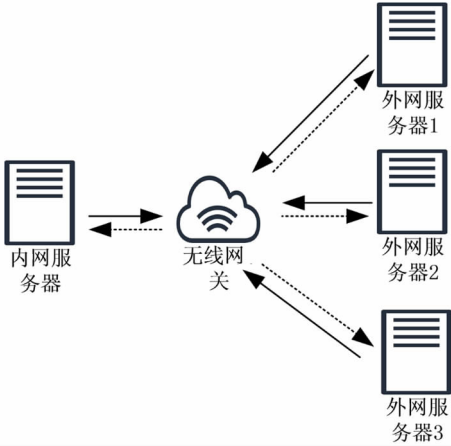


图 1 测试平台网络结构示意图

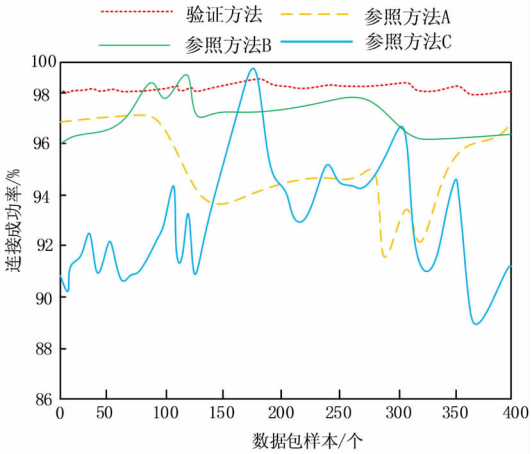


图 2 不同方法获得的连接指标对比图

2.3 连接偏差测试

基于上述测试条件及其测试数据,对参照方法进行连接偏差测试,在测试条件不变的情况下,每 20 组连接为 1 轮,共计 20 轮测试,得到每种方法的 20 组连接偏差值,具体结果如表 2 所示。对比偏差指标大小,得出测试结论。

观察表 2 数据可以发现,每种方法所得指标各不相同,且每种方法所得相邻指标之间差值均小于 0.1。按照测试标准对比参照方法 A、参照方法 B、参照方法 C 与验证方法偏差指标值大小可知,验证方法指标值最小,其项是参照方法 B,参照方法

C 排列其后,参照方法 A 偏差值最大。因此验证方法的连接效果最好,偏差最小。

测试组	连接偏差指数			
	参照方法 A	参照方法 B	参照方法 C	验证方法
第 1 轮	0.86	0.72	0.82	0.59
第 2 轮	0.87	0.74	0.75	0.64
第 3 轮	0.84	0.72	0.86	0.63
第 4 轮	0.87	0.68	0.84	0.59
第 5 轮	0.86	0.64	0.86	0.64
第 6 轮	0.87	0.68	0.75	0.63
第 7 轮	0.92	0.71	0.74	0.62
第 8 轮	0.90	0.73	0.73	0.68
第 9 轮	0.87	0.68	0.77	0.67
第 10 轮	0.87	0.72	0.82	0.62
第 11 轮	0.86	0.72	0.75	0.68
第 12 轮	0.87	0.74	0.86	0.64
第 13 轮	0.87	0.72	0.82	0.62
第 14 轮	0.86	0.68	0.75	0.58
第 15 轮	0.87	0.64	0.82	0.59
第 16 轮	0.87	0.68	0.75	0.64
第 17 轮	0.86	0.71	0.86	0.63
第 18 轮	0.87	0.64	0.84	0.62
第 19 轮	0.92	0.68	0.86	0.68
第 20 轮	0.90	0.71	0.75	0.67

2.4 抗扰性测试

为了验证提出的方法具有良好的抗扰性,在非信任内网区域与信任区域连接的无线网络环境下,释放随机扰动信号,在保证参测方法能够成功连接的情况下,记录每种方法的信号扰动状态,并生成信号波形图,如图 3~图 6 所示。对比信号信噪比大小,得出测试结论。

通过对比图 3~6 信号波形可以发现,参照方法 A 在扰动信号混淆影响下,其方法抗扰效果薄弱,噪声波形明显,信噪比指数较大;参照方法 B 的信号前段与部分中段噪声抑制或滤除效果良好,但部分中段与末端信号噪声仍然存在,因此抗扰效果并不理想;参照方法 C 的信号部分中段信号可以看出对应噪声的收敛效果,但是前段与末端信号噪声扰动明显,故此抗扰效果存在不足;验证方法波形相比上述三种波形收敛效果明显,且噪声扰动痕迹滤除较彻底,结合信噪比指标可以判定验证方

法的抗扰性最好。

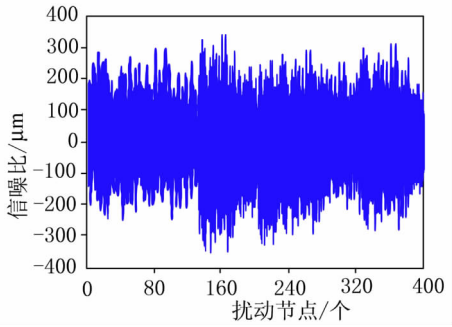


图 3 参照方法 A 连接扰动信号情况

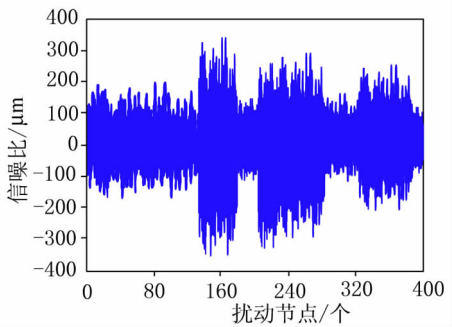


图 4 参照方法 B 连接扰动信号情况

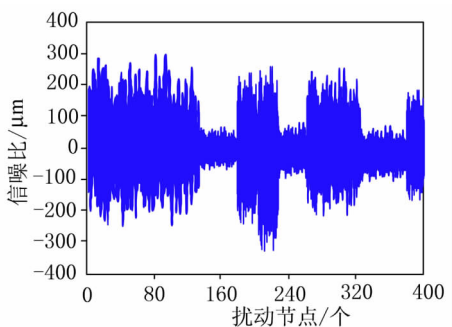


图 5 参照方法 C 连接扰动信号情况

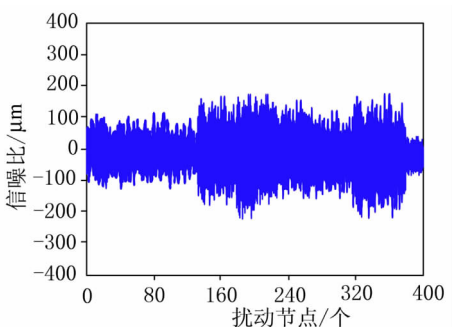


图 6 验证方法连接扰动信号情况

3 结 论

从非信任内网区域与信任区域信任值入手,对

其所在区域节点进行优化,改变连接环境,进而提升连接成功率与安全系数。方法的提出与实现,对无线通信网络安全研究具有推动作用。但是,受到当前大数据、AI 技术等数据技术形态的影响,数据连接方式不断更新,连接风险仍然存在。为了使提出方法具有更好的适应性与最佳的连接效果,需要通过不断积累网络数据,构建不同网络环境的连接节点训练模型,通过尝试引入 AI 学习算法,提升方法连接安全策略,完善模型自适应安全体系,确保方法的高效、准确、稳定。

参考文献

[1] 任伟峰. 内网敏感大数据共享交换安全性监控平台设计[J]. 信息技术,2022(10):118—123.

[2] 韩磊,李洋,任新. 网络准入控制中的内网安全防护方案探讨[J]. 信息系统工程,2022(10):88—91.

[3] 刘宇萌. 基于深度学习的无线通信网络数据安全态势感知研究[J]. 信息记录材料,2022,23(8):182—185.

[4] 贺云龙,梁其才,曾维鹏. 内网信息安全策略与技术研究[J]. 软件,2022,43(8):101—103.

[5] 赵军岩. 网关互连 CAN 网络中的消息最坏响应时间分析研究[D]. 长沙:湖南大学,2015.

[6] 沈冬远,武丹丹. 一种基于连接和安全熵的网络空间整体安全认识和方法[J]. 信息安全与通信保密,2022(6):135—143.

[7] 梁振宇. 基于计算机技术的无线通信网络安全风险预测研究[J]. 河南科技,2022,41(10):16—19.

[8] 李寒箬. 内网中的信息安全防御系统设计与实现[J]. 集成电路应用,2022,39(5):120—121.

[9] 蒋志顺,范雷. 基于机器学习的无线通信网络安全漏洞智能监测系统[J]. 电子设计工程,2021,29(15):115—119.

[10] 王增兴. 互联网时代公共无线通信网络安全存在的问题及对策[J]. 信息与电脑(理论版),2021,33(14):205—207.

[11] 王柳彬. 基于无线协作通信网络的物理层安全技术研究[D]. 重庆大学,2021.

[12] 杨光,王顺新,李俊喜. 无线通信网络的安全问题及防范策略研究[J]. 网络安全技术与应用,2021(3):67—68.

[13] 许丹. 无线通信网络物理层安全技术研究[D]. 杭州电子科技大学,2021.

[14] 程梓豪. 无线通信网络中的隐蔽监控与安全传输研究[D]. 西安电子科技大学,2021.

[15] 李冰,李钊,李建军,等. 一种可信网络模型的构建方法[J]. 无线电通信技术,2012,38(3):20—22+42.

(上接第 158 页)

而补偿前则至少需 30 s 才能达到平稳效果,这是因为该方法引入了状态转移矩阵和牛顿力学运动方程,进行增益矩阵的更新处理,对智能机器人位置进行不断预测修正,可有效提升 IMU 航向角控制的稳定性,控制效率高,可助力提升换流站设备巡检效果。

3 结 论

以某地区换流站为实验目标,将本文方法应用于智能机器人的巡检任务中,通过分析多传感器数据融合前后的巡检误差、IMU 航向角的误差补偿效果等验证本文方法的实用性,实验结果表明:本文方法具有巡检避障能力,定位误差仅为厘米级;能实现 IMU 航向角误差的补偿。

参考文献

[1] 何志甘,范彦琨,付胜宪,等. 柔直换流站阀厅巡检机器人巡检路径规划[J]. 集成电路应用,2021,38(2):50—51.

[2] 张雪姝,伦振坚,侯婷,等. $\pm 800\text{kV}$ 柔直换流站全封闭阀厅智能巡检系统研究[J]. 南方能源建设,2019,6(4):144—151.

[3] 朱添益,戴逢哲,康文,等. 直流换流站运维监控系统智能机器人设计方法[J]. 电气技术,2020,21(2):22—25.

[4] 黄俊波,蔡澍雨,贾永祥. 基于虚拟现实技术在无人机巡检输电线路的研究[J]. 电子测量技术,2020,43(8):38—41.

[5] 袁虎强,苏志龙,蒋新华,等. 基于多旋翼无人机的特高压换流站设备巡检路径规划[J]. 电子设计工程,2021,29(12):157—160+165.

[6] 李帅鑫,李广云,王力,等. LiDAR/IMU 紧耦合的实时定位方法[J]. 自动化学报,2021,47(6):1377—1389.

[7] 张福斌,张炳烁,杨玉帅. 基于单目/IMU/里程计融合的 SLAM 算法[J]. 兵工学报,2022,43(11):2810—2818.

[8] 任金伟,郑鑫,李昱辰,等. 基于新型多传感器融合策略的移动端双目视觉惯性 SLAM 闭环算法研究[J]. 高技术通讯,2021,31(7):681—691.

[9] 王通典,刘洁瑜,吴宗收,等. 基于多尺度光流融合特征点视觉—惯性 SLAM 方法[J]. 系统工程与电子技术,2022,44(3):977—985.

[10] 章弘凯,陈年生,代作晓,等. 一种多层次数据融合的 SLAM 定位算法[J]. 机器人,2021,43(6):641—652.

[11] 蔡英凤,陆子恒,李祎承,等. 基于多传感器融合的紧耦合 SLAM 系统[J]. 汽车工程,2022,44(3):350—361.

[12] 王铉彬,李星星,廖健驰,等. 基于图优化的紧耦合双目视觉/惯性/激光雷达 SLAM 方法[J]. 测绘学报,2022,51(8):1744—1756.

[13] 孙楠,裴信彪,王春军,等. 基于立体视觉——惯导 SLAM 的四旋翼无人机导航算法[J]. 微电子学与计算机,2020,37(5):33—38+42.

[14] 朱朔凌,毛建旭,王耀南,等. 基于惯性导航角度补偿的室内激光 SLAM 方法[J]. 电子测量与仪器学报,2019,33(3):1—7.

[15] 耿越,雷旭升. 基于分量信息融合的扩展卡尔曼滤波算法[J]. 计算机仿真,2019,36(7):239—243.