• 医学信息技术 •

智慧医院物联网系统可信度研究及分析*

胡 佳 许 蓉 陶新娟 蒋 恒

(岳阳市人民医院信息科 岳阳 414000)

〔摘要〕 介绍物联网系统可信度评估常见方法，提出物联网系统异常检测体系架构和可信度评估规范，在实验基础上阐述物联网内外部因素可信度分析方法、物联网系统可信度评估方法，分析实验结果。

〔关键词〕 物联网；可信度；异常检测；电磁环境

〔中图分类号〕R-058 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673-6036.2022.06.012

Study and Analysis on the Credibility of Internet of Things System in Smart Hospital *HU Jia, XU Rong, TAO Xinjuan, JIANG Heng, Department of Information, Yueyang People's Hospital, Yueyang 414000, China*

〔**Abstract**〕 The paper introduces common methods for reliability evaluation of Internet of Things (IoT) system, proposes abnormal detection architecture and reliability evaluation specifications of IoT system, expounds reliability analysis methods of internal and external factors of IoT and reliability evaluation methods of IoT system on the basis of experiments, and analyzes experimental results.

〔**Keywords**〕 Internet of Things (IoT); reliability; abnormal detection; electromagnetic environment

1 引言

1.1 物联网系统可信度评估常见方法

近年来物联网（Internet of Things，IoT）逐渐广泛应用于不同领域，催生了智能基础设施概念，如智能计量系统、智慧城市、智能电网等。在智慧医院物联网系统中传感器收集患者及环境数据并发送到 Sink 汇聚节点上，Sink 节点使用路由协议将数据转发到边界路由器或云服务器。由于具有安全特性或任务特性，物联网系统必须在整个预期任务时间内可信运行。可信度是物联网应用的关键要求之一[1]。推荐信任模型一般从邻居节点收到推荐，恶意节点可能会发送错误推荐，从而导致合法节点获得较低的信任值[2]。有研究者使用直接信任作为可信度[3]，这种方法的主要问题是节点看似正常工作，但可能发送错误建议。CORE 方法[4]使用看门狗机制计算可信度，该方法仅交换积极参数，以限制移动节点恶意性质传播行为。CONFIDENT 方法[5]使用直接和间接建议计算可信度，并使用报警消息识别恶意节点或系统。SORI 方法[6]使用直接观察和基于推荐的机制计算可信度，根据节点可信度值以概率方式丢弃数据包。上述 3 种方法存在隐患，即对象可能表现良好但是会发送错误建议。TWSN[7]方法使用相似性机制计算推荐人的可信度，

〔修回日期〕 2021-09-28

〔作者简介〕 胡佳，博士，高级工程师，发表论文 7 篇。

〔基金项目〕 国家自然科学基金课题“开源社区项目合作关系深度学习推荐方法研究”（项目编号：61802120）；湖南省自然科学基金课题“开源社区项目合作关系深度学习预测方法研究”（项目编号：2019JJ50018）。

使用基于均方根的模型将建议与个人经验相关联。有学者[8]提出物联网边缘设备信任机制，该方法的总体信任基于设备到设备之间的直接信任和来自代理的反馈信任进行计算，其最大问题在于反馈信任的正确性取决于信息流后端节点的可信度，而有时无法评估其可信度。

1.2 研究内容

本文通过分析物联网内外部的可信度因素，设计一种度量方法量化系统中不当行为的数量，作为衡量可信度的手段，从而动态调整设备信任度，保护数据的安全性和准确性；引入宽恕概念的群信任计算规范，来计算监测患者健康的一组传感器的可信度和对患者的总体风险，更准确地评估数据中心收到的数据。

2 物联网内外部可信度分析

2.1 物联网外部电磁环境的可信度分析

2.1.1 电磁噪声源 医疗环境中的电磁噪声源包括常见的电力装置、电子医疗设备、进入建筑物的物体发出信号以及建筑物外产生的侵入建筑物的无线电波或电磁场。微波治疗设备、安装在病房里的微波炉和加热器发出的电磁噪声与 ISM 频段相同。还有被带进医院的问题物品，包括手机、Wi－Fi 路由器和带有通信设备的游戏机。此外 LED 灯电路板电磁场泄露会导致放置在天花板附近的医学监测系统被无线电干扰[9]。当使用物联网系统时必须仔细考虑消除电磁噪声源的方法。

2.1.2 影响信号传播的因素 包括建筑结构组成部分，如墙壁、地板、门、窗户以及金属柜等固定装置。对墙壁和天花板表面进行检查是不够的，因为内壁组成可能与表面有很大不同。空调系统的金属管道经常被放置在病房的天花板上，可能影响信号传播。在实施过程中应该在与医院员工广泛讨论的基础上小心处理上述问题。

2.1.3 优化电磁场环境 如果物联网系统使用无线通信则必须对系统运行区域的电磁环境进行良好维护，不仅需要了解建筑材料，还需要利用屏蔽吸收技术控制医院电磁场。可以通过放置反射器和吸收器阻止信号侵入。但是医院大楼被完全屏蔽，移动电话和公共 Wi－Fi 等公共通信信号将无法到达大楼内部终端。有文献[10]提出非金属周期结构在特定频率的选择性屏蔽方面具有广阔应用前景，并提出带阻屏蔽技术解决方案，即将光子晶体的带隙特性应用于改变结构尺度的微波区域。图 1 显示了一个二维周期结构，其由平行交叉的电介质板组成。根据文献[10]，本文的一些参数设置如下：单元格大小为 1.25 毫米（对角线长），时间槽取值为 2.5 皮秒，通道管径为 2.5 毫米，相邻通道管距离为 10 毫米，相对介电系数为 8.9，电磁波特性为横向正弦电磁波。图 2 给出时域有限差分（Finite Difference Time Domain，FDTD）仿真得到的电磁波屏蔽效应的频率特性。其中纵轴表示非周期结构时的电场变化率，随着层数的增加无线局域网 5GHz 频段的电磁波可以得到有效衰减。

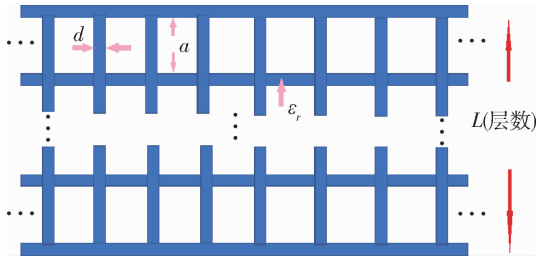

图 1 二维非周期结构示例（平行交叉的电介质板）

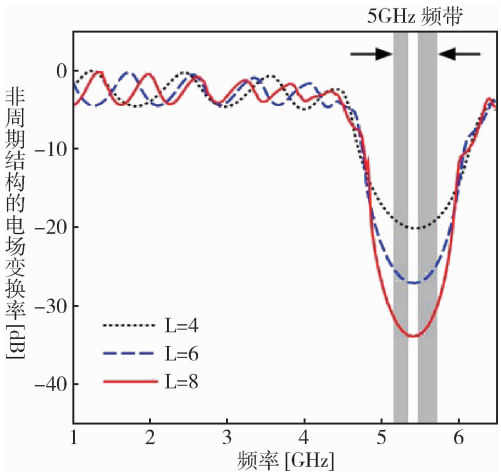

图 2 非周期结构的横向电磁波频率特性[10]

2.2 物联网系统内部高效的异常检测体系架构（图3）

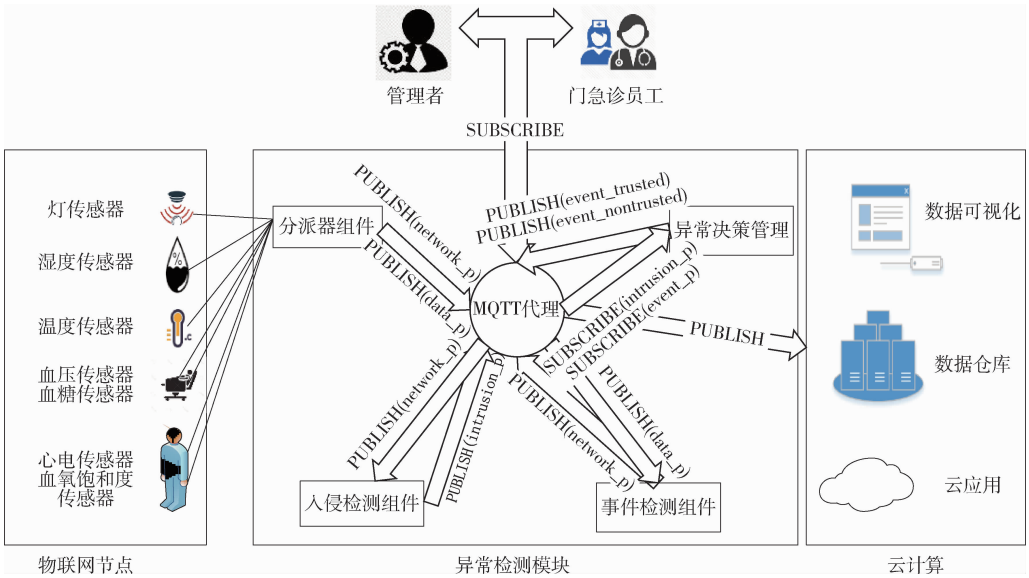

图3 异常检测模块的体系结构及主要组成部分

2.2.1 分派器组件 分派器组件充当包过滤器，从不同传感器节点接收到的数据包都在分派器组件上进行处理，主要包括提取、标准化和发布收集到的两类数据，即网络数据和传感器采集数据。

2.2.2 入侵检测组件 该组件检测网络状态异常，订阅与网络数据相关的主题，包括分派器组件过滤和消息队列遥测传输（Message Queueing Telemetry Transport，MQTT）发布的网络数据。采用支持向量机（Support Vector Machine，SVM）算法对接收到的数据进行分类。一旦建立识别模型，机器学习算法有能力检测出未知的新形式攻击。在物联网中常见的有 Rank 攻击、泛洪攻击、版本号修改攻击。

2.2.3 事件检测组件 此组件检测与环境和患者健康状态相关的异常。分散在医院内的不同传感器将数据发送到边界路由器。该组件订阅传感器数据主题以接收由分派器组件过滤的除与网络相关外的所有数据。与入侵检测组件一样 SVM 用于检测感兴趣事件，这些事件由相关人员实时接收。

2.2.4 异常决策管理 与患者生命健康有关的数据非常重要，入侵可能修改数据，导致应急人员做出不恰当决定。因此当异常决策管理器收到来自入侵检测组件或事件检测组件的通知时，会按照相关评估规则计算信任度而做出相应反应。当信任度低于阈值时异常决策管理将在事件数据上添加标签（不受信任），提醒医务人员接收的数据可能是伪造的。当网络管理员修复问题后系统恢复正常状态，事件数据被标记为可信。

2.2.5 MQTT 代理 MQTT 是一种使用发布/订阅原则、用于物联网应用的轻量级消息传输协议。组件连接到 MQTT 代理服务器并以松耦合方式交换信息。因此分派器组件在收到来自节点的消息后发布网络参数（n_ p）和数据参数（d_ p）。入侵检测组件和事件检测组件订阅这些参数并通过发布入侵参数（i_ p）和事件参数（e_ p）检测异常，根据可信任度评估规范计算设备可信度。

3 物联网系统可信度评估

3.1 概述

假设在医院物联网场景中患者安装了无线传感器，所有传感器生成数据都由节点发送到分派器组件，该组件将数据上报至 MQTT 代理，分发至相应节点。这些设备可能周期性地受到设备功能方面

（不会导致数据异常）或恶意活动（会导致数据偏离正常值和期望值）影响。其中功能方面影响包括设备硬件故障、低电量问题、通信信道干扰等；恶意活动影响包括可改变数据或中断数据传输的任何类型的主动攻击。

3.2 评估方法

3.2.1 典型的信任评估方法 公式（1）表示设备异常行为的聚合方法，W 用于分配功能方面的异常活动权重，$(1-W)$ 用于分配一段时间内设备恶意活动的权重。

$$A_A(t) = W \times \sum_1^n F_e + (1-W) \times \sum_1^n O_e \quad (1)$$

对于影响设备运行可忽略不计的情况，如患者移动引起的通信信道干扰，整合安全的两个基本属性：宽恕和基于实体的可信度评估。宽恕是指如果一个实体在一段时间内没有行为不端，那么会提高这个实体的信任度，停止恶意行为的设备会得到奖励。考虑这两种安全性属性，公式（2）通过引入宽恕的概念和奖励在一段时间内没有恶意的实体来增加信任。r 为控制宽恕率的经验因子，b_r 是信任值下降到极点再到提高至阈值所需时间，t_p 是自异常活动的前一条记录以来所经过的时间。公式（3）是信任度惩罚偏差计算规范，一般以 2 为底数代表该系统更保守。公式（4）将信任以公式（3）中计算的偏差递减。值得注意的是，信任是以负值计算的，因为异常活动降低了实体可信度。

$$T_D(t) = r^{\frac{t\_p}{b\_r}} \times |T(t-1)| \quad (2)$$

$$\Delta T = \log_2 T_D(t) \times A_A(t) \quad (3)$$

$$T(t) = T(t-1) - \Delta T \quad (4)$$

3.2.2 引入群信任概念进行评估 典型的信任评估方法集中在单个设备上并对其行为进行分级。由于可以在患者身上安装许多设备，引入群信任概念，作为评估特定患者的一组设备可信度的方法。间接地，群信任反映了存在不当行为时恰当评估患者健康的相关风险。为了正确计算群信任，引入基于患者所治疗疾病的设备加权信任思想。如发热患者体温传感器所收集数据比氧饱和传感器所收集数据更为关键。因此使用加权信任概念，将每个设备的信任值乘以一个特定权重，所有权重之和等于 1。通过考虑设备在其行为不端的实例上加权信任值来描述群信任，得到公式（5）和（6）：

$$G_T = (a \times T_{An}) + (b \times T_{An-1}) + (c \times T_{An-2}) \quad (5)$$

$$T_{An} = (W_{c_x} \times T(t)_x)_n \quad (6)$$

4 实验结果及分析

4.1 异常检测系统有效性

4.1.1 有效性验证方法 为验证本文提出的异常检测方法的有效性，采用入侵检测数据集和事件检测数据集并使用 Contiki - Cooja 模拟器实现一个异常场景。其中入侵检测数据集与网络的正常行为相关，事件检测数据集分为两类：环境数据集和人体数据集。使用温度、光和湿度数据值模拟火灾场景，使用心率、血压和体温模拟人体数据采集。为了验证算法，通过减少心率数据模拟心脏病发作场景。

4.1.2 异常检出率（Abnormal Detection Rates，ADR） 评估所提方法的性能，ADR 用于识别在某时间段内的异常事件的检出率。ADR 定义如下：

$$ADR = \frac{ADR\ by\ SVM}{Total\ data\ amount} \quad (7)$$

入侵检测模块检测到两种 ADR 较高的路由攻击（ADR 均高于 90% 的 Rank 攻击和版本号修改攻击）。以较低的 ADR 检测泛洪攻击。这可以从模拟器在泛洪攻击后恢复正常状态的对策中得到解释。通过对温度、心率的异常检测，正确检测出火灾和心脏病发作的异常情况，见表 2。

表 2 入侵检测和事件检测的异常检出率

异常检测项目	ADR（%）
Rank 攻击	94.5
泛洪攻击	63.8
版本号修改攻击	92.1
温度升高	84.3
心率降低	87.6

4.2 系统信任度评估

4.2.1 设备信任评估 为了便于验证，活动是根据事件之间上限和下限随机生成，每个活动的数量

根据预先分配的权重控制。血压传感器和体温传感器异常活动数量较少，是更值得信赖的设备。心电图和血氧饱和度显示出更多异常活动并向下移动到一个更小的信任值。对于群信任图，取的信任值进行加权，心电取 0.5 权重，血氧取 0.3 权重，其余取 0.1 权重，群信任的方向更接近心电传感器的行为。

4.2.2 引入宽恕的信任评估 当设备出现故障时，更重要的信任设备可信度突然发生变化，导致整体信任度发生剧烈变化，这时数据不应该再被信任。没有引入宽恕策略时，随着时间的推移，即使设备恢复正常，但已被打上不可信的标签导致整体信任度依旧不能升高，这与实际情况不符。引入宽恕策略后，群信任改善，接近实际结果。采用宽恕策略，随着时间的推移只要没有任何不当行为对设备的信任度就可以提高，设备可以值得信任。

5 结语

本文从内外部因素研究已用于医院物联网部署场景的信任评估，以监测和协助住院患者护理。通过实验仿真得知关注引入宽恕策略的群信任会对物联网系统提供更准确的可信评估。本研究根据故障和异常活动的类型分配权重来区分设备不同类型的异常行为，更好地提示设备故障影响患者健康相关的风险。更重要的是，将测量患者健康的关键因素设备适当地集成到信任模型中，以便更好地评估信任并减轻患者相关风险。

参考文献

1 Pasricha Sudeep. Overcoming Energy and Reliability Challenges for IoT and Mobile Devices with Data Analytics [C]. Pune: 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID), 2018.

2 Niyato D, Hossain E, Kim D I. Wireless - Powered Communication Networks (Architectures, Protocols, and Applications). Mobile Ad - Hoc Networks and Delay - Tolerant Networks with Wireless Energy Harvesting [M]. Cambridge: Cambridge University Press, 2017: 383 - 429.

3 Govindan K. Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey [J]. IEEE Communications Surveys & Tutorials, 2011, 14 (2): 279 - 298.

4 Pietro Michiardi, Refik Molva. Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks. Advanced Communications and Multimedia Security [M]. Boston: Springer, 2002: 107 - 121.

5 Buchegger S, Boudec J. Performance Analysis of the CONFIDANT Protocol [C]. Lausanne: Proceedings of the 3rd ACM International Symposium on Mobile ad Hoc Networking & Computing, 2002.

6 He Q, Wu D, Khosla P. SORI: A Secure and Objective Reputation - based Incentive Scheme for ad - hoc Networks [C]. Atlanta: 2004 IEEE Wireless Communications and Networking Conference, 2004.

7 Reddy V B, Negi A, Venkataraman S. Communication and Data Trust for Wireless Sensor Networks Using D - S Theory [J]. IEEE Sensors Journal, 2017, 17 (12): 3921 - 3929.

8 Yuan J, Li X. A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi - Source Feedback Information Fusion [J]. IEEE Access, 2018 (6): 23626 - 23638.

9 Ishida K, Gotoh K, Hirose M. Electromagnetic Compatibility of Light - Emitting Diode (LED) Lamps and Wireless Medical Telemeters [C]. Białystok: XXIV International Conference on Electromagnetic Disturbances, 2017.

10 Kudou T, Hanada E. Numerical Analysis of Electromagnetic Band - stopping Using Non - metal Periodic Structures [C]. Seoul: 2016 URSI Asia - Pacific Radio Science Conference (URSI AP - RASC), 2016.