软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(7):1922−1936 [doi: 10.13328/j.cnki.jos.005360]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于恶意读写器发现的 RFID 空口入侵检测技术*

黄伟庆[1,2,3], 丁 昶[2,3], 崔 越[2,3], 王思叶[1,2,3], 张艳芳[2,3], 赵博白[2,3], 诸邵忆[2,3], 毛 锐[2,3], 陈 超[2,3]

[1](北京交通大学 计算机与信息技术学院,北京 100044)

[2](中国科学院 信息工程研究所,北京 100093)

[3](中国科学院大学 网络空间安全学院,北京 100093)

通讯作者: 王思叶, E-mail: wangsiye@iie.ac.cn

摘 要: 随着 RFID 技术的不断发展,其在物流管理、货物监控、会议安全保障等领域的应用越来越广泛,但随之而来的安全威胁是不得不需要考虑的隐患因素.在无线通信技术中,空中接口定义了终端设备与网络设备之间的电磁连接技术规范.目前大部分 RFID 设备采用公开的标准通信协议进行数据传输,使得 RFID 系统容易遭到恶意设备的空口入侵,从而导致 RFID 系统面临严重的安全威胁与数据隐私保护问题.研究基于恶意读写器的实时发现,完成空口入侵的检测,避免空口数据遭到窃取,保证数据传输安全.主要利用无源感知技术对 RFID 信号无线信道状态信息进行分析与计算,综合运用接收信号强度、相位、吞吐量等信息,提取并建立可以描述无线信道状态信息的参数.利用提取的参数建立基于有限状态机的 RFID 信号感知数据推断模型,结合自适应算法得出稳态作为依据,分析判断 RFID 信号的具体变化,实现基于恶意读写器的 RFID 空口入侵检测.

关键词: 物联网安全;无源 RFID;空口入侵;隐私保护

中图法分类号: TP309

中文引用格式: 黄伟庆,丁昶,崔越,王思叶,张艳芳,赵博白,诸邵忆,毛锐,陈超.基于恶意读写器发现的 RFID 空口入侵检测技术.软件学报,2018,29(7):1922−1936. http://www.jos.org.cn/1000-9825/5360.htm

英文引用格式: Huang WQ, Ding C, Cui Y, Wang SY, Zhang YF, Zhao BB, Zhu SY, Mao R, Chen C. RFID air interface intrusion detection technology based on malicious reader discovery. Ruan Jian Xue Bao/Journal of Software, 2018,29(7): 1922−1936 (in Chinese). http://www.jos.org.cn/1000-9825/5360.htm

RFID Air Interface Intrusion Detection Technology Based on Malicious Reader Discovery

HUANG Wei-Qing[1,2,3], DING Chang[2,3], CUI Yue[2,3], WANG Si-Ye[1,2,3], ZHANG Yan-Fang[2,3], ZHAO Bo-Bai[2,3], ZHU Shao-Yi[2,3], MAO Rui[2,3], CHEN Chao[2,3]

[1](School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China)

[2](Institute of Information Engineering, The Chinese Academy of Sciences, Beijing 100093, China)

[3](School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100093, China)

Abstract: With the continuous development of RFID technology, its applications in logistics management, cargo monitoring, conference security and other fields are becoming broader and broader. In wireless communication technology, the air interface defines the technical specification of the radio link between the terminal device and the network device. Most of the current RFID devices use common standardized communication protocol for data transmission, which makes the RFID systems suffer air interface intrusion by malicious devices. The air interface intrusion can then cause the security threats and data privacy protection problem in RFID systems. This study

* 基金项目: 国家高技术研究发展计划(863)(2013AA014002)
Foundation item: National High Technology Research and Development Program of China (863) (2013AA014002)
本文由“面向隐私保护的新型技术与密码算法”专题特约编辑刘吉强教授推荐.
收稿时间: 2017-05-29; 修改时间: 2017-07-13; 采用时间: 2017-08-22; jos 在线出版时间: 2017-10-17
CNKI 网络优先出版: 2017-10-17 13:38:04, http://kns.cnki.net/kcms/detail/11.2560.TP.20171017.1338.007.html

accomplishes the detection of air interface intrusion based on the real-time discovery of malicious readers. It avoids theft of data and ensures the security of data transmission. The paper mainly uses passive sensing technology for the analysis and calculation of the RFID signal, channel state and throughput information. Parameters are extracted from the received signal strength, phase and other state information to describe the wireless channel state. The extracted parameters and finite-state machine theory are used to build a perception data inference model of RFID signal and to obtain an initial steady state according to the adaptive algorithm. As a result, the specific change of RFID signal can be analyzed to complete the detection of RFID air interface intrusions.

Key words: security of IoT; passive RFID; air interface invasion; privacy protection

由于网络技术及传感设备的发展,物联网在人们的生活中占据了重要位置.作为物联网技术的重要组成部分,RFID(radio frequency identification,射频识别)技术凭借其短时延、高精度、非接触、非视距、成本低和传输范围大等优点,已经成为室内环境中监控系统普遍采用的主流技术,在民用与军用领域得到了广泛应用,发挥着至关重要的作用[1−3].

目前较为常用的 RFID 设备工作的频段分为 HF 频段(13.56KHz)、UHF 频段(925MHz)与微波频段(2.4GHz),其中,UHF 频段凭借其检测范围广、读取速率快，识别效率高等优势被大量应用于 RFID 系统中,本研究主要面向室内环境中 UHF 频段无源 RFID 设备进行.已知 RFID 标签数据通过无线射频与读写器进行通信,目前的 RFID 通信协议保证了不同厂家读写器读取标签数据的通用性,但同时也导致 RFID 系统无法拦截恶意读写器对标签数据的识读[4−7].RFID 空中接口入侵检测是指通过收集 RFID 系统空中接口数据信息并对其进行分析,从中发现系统或环境中是否有违反安全策略的行为或被攻击的情况.如图 1 所示,如果系统对数据在空中接口传输过程中不进行有效的入侵检测与保护,攻击者很可能利用恶意读写器截获空口数据,对 RFID 系统进行干扰和破坏,使 RFID 系统面临严重的安全威胁与数据隐私保护问题,产生的安全风险具体如下.

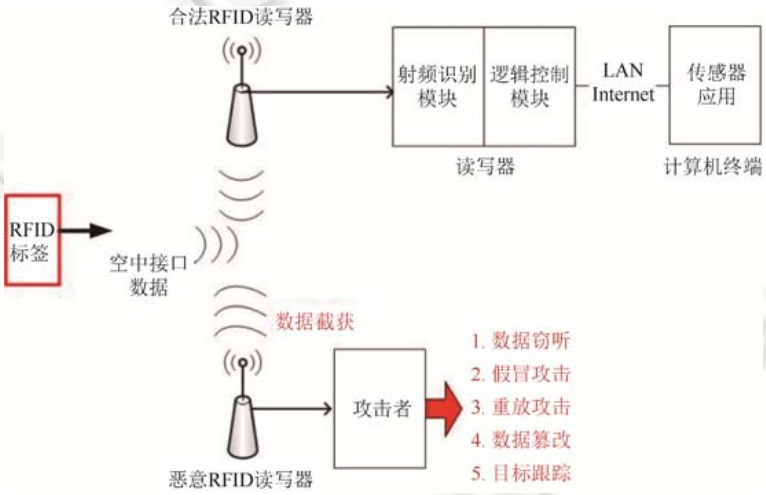

Fig.1 The threaten of RFID air interface data interception

图 1 RFID 空口数据截获威胁示意图

(1) 数据窃听:加密密钥被截获的风险.无线信道是一个开放性信道,任何具有适当的无线设备的人都可以通过窃听无线信道而获得信息.以目前我国的国标和国军标为例,基于密码算法的安全协议长时间使用相同的密钥,如果被恶意读写器获取会带来极大的安全隐患.

(2) 假冒攻击:克隆或者伪造标签的风险.主动攻击者利用恶意读写器假冒合法 RFID 读写器,获取大量合法用户的身份、数据信息,制造具有相同编码的标签,由于目前通用 RFID 协议,如 EPC、ISO 等并没有规定对标签进行认证,故读写器无法鉴别克隆标签的真伪.

(3) 重放攻击:主动攻击者将窃听到的有效信息经过一段时间以后再次传给信息的接收者,以骗取系统的

信任,达到其攻击的目的.

(4) 数据篡改:主动攻击者将接收到的信息进行修改,如删除或替代部分或全部信息之后,再将信息传给原本的接收者.由于目前 RFID 协议没有规定标签对读写器的认证,攻击者可以利用兼容的读写器通过写指令来篡改标签的信息.

(5) 目标跟踪:数据隐私泄露风险.RFID 标签以明文的形式发送 EPC 编码,故当攻击者具有一台普通的兼容该协议的读写器并靠近标签时,即可获得标签的编码.由于该编码的唯一性,攻击者通过获取 EPC 编码可能分析出目标的位置与个人信息等数据,造成隐私泄露的风险.

基于恶意读写器的实时动态发现,实施对 RFID 空中接口的入侵检测,可以有效降低 RFID 系统空口数据传输通信面临的安全风险,对保障 RFID 系统的安全性,提高系统的数据隐私保护能力有着重大的意义.

本研究主要围绕以下几项内容展开.

(1) 研究室内空间中 RFID 无线信号的传输特性,分析 RFID 信号在室内环境中的传播变化规律,根据 RFID 信号的信道传播特性,总结读写器干扰类型,分析恶意 RFID 读写器对合法 RFID 系统的影响情况;

(2) 研究恶意 RFID 读写器对合法 RFID 读写器的影响范围,设计建立恶意读写器判别模型和度量参数,同时通过测试分析,提取度量参数的具体表示指标;

(3) 最后,基于有限状态机原理设计判别模型的实现方法,计算判别模型的判断条件及其置信区间,实现室内环境中 RFID 空口入侵的快速动态检测,并评估入侵检测方法的实时性与准确性.

1 国内外现状及发展动态分析

如图 2 所示,目前通用的无源 UHF 频段 RFID 系统结构主要由 3 部分组成:读写器(reader)、电子标签(tag)和后端系统,其中读写器一般与对应的天线(antenna)连接进行信号发送与接收.RFID 读写器通过调制射频信号向标签发送编码信息和连续载波.标签一方面从接收到的射频信号中解调出有用信息,另一方面从读写器发射的连续载波中获得自身的驱动能量,并且标签通过调节天线的反射阻抗系数来完成对 RFID 读写器信息的传送.

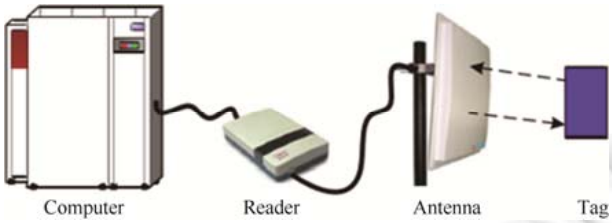

Fig.2 RFID system components

图 2 射频识别(RFID)系统基本组成

根据 RFID 技术的自身特点和工作原理,目前针对 RFID 空中接口数据防护的方法主要包括:数据加密、专有安全协议设计、RFID 空口入侵检测等.

数据加密方法通过加密算法对 RFID 标签与读写器间的通信数据进行加密,使恶意 RFID 读写器无法解析数据,从而保证空口数据的安全性.文献[8]提出基于最小密码技术的算法实现对空口数据的保护;文献[9]采用对称密码机制,防止攻击者获取标签中信息的真实含义,以此提高空口数据的安全性;文献[10]基于公钥密码技术提出了重加密技术,很好地解决了位置隐私泄露问题,但该技术需要进行密钥管理,提高了系统成本.文献[11]提出了统一重加密(universal re-encryption technology)算法进行空口数据保护,算法基于 ElGamal 密码体制,基本原理与重加密技术相似,具有多个私钥/公钥对,实现了空口传输数据的语义安全.

在 RFID 的安全协议方面,针对现有协议的安全漏洞,国内外学者提出了一系列改进的安全协议.文献[12]提出了一种基于 Hash 函数与密钥更新的 RFID 双向安全认证协议.该协议可有效抵抗重放攻击、跟踪攻击、

假冒攻击、阻断和篡改攻击,同时在协议的计算复杂度方面得到了较好的兼顾.文献[13]提出一种抗去同步化的轻量级 RFID 双向认证协议.该协议能够有效抵抗位置跟踪攻击、标签伪造,并可保证前向安全和后向安全.文献[14,15]基于 SRP 协议,提出 SRP+协议与 SRP++协议,可以抵抗可抵御假冒标签、假冒读写器、失同步攻击以及跟踪攻击.文献[16]提出了基于分组共享密钥的 RFID 标签批认证协议方案,实现对标签信息的隐私保护和抗 DDos 攻击,方案具有较高的计算效率与较低的系统开销.

在 RFID 空口入侵检测研究方面,文献[17]提出利用监视读写器(watchdog reader)的方法,采集系统工作时的标签读取次数,发现标签读取数据的异常,进而实现对 RFID 空中接口的入侵检测.由于需要增加附加的 RFID 读写设备,因此该方法成本较高.文献[18]利用模糊聚类的方法,首先采集正常 RFID 空口数据进行训练与特征提取,随后将系统采集数据进行分析测试,实现异常数据的发现和 RFID 空口入侵检测.该方法无需附加硬件设备采集数据,但是由于需要进行前期训练,因此实时性较差.同时,训练模型对检测结果影响较大,导致该方法检测准确度稳定性较差.文献[19]利用非单调推理方法对 RFID 系统采集的数据进行分析,发现异常冲突数据,从而实现对 RFID 空口的入侵检测,该方法主要针对克隆标签对 RFID 空中接口的入侵情况,无法对恶意读写器进行发现,应用范围较为单一.文献[20]提出基于免疫网络的 RFID 空口入侵检测模型,利用生物学中的免疫模型将采集的信道数据进行还原并与 RFID 系统中数据进行对比分析,实现对 RFID 空口的入侵检测.由于该方法需要增加专用的信号采集设备,因此成本较高.

针对实际环境中恶意读写器发现的研究,目前主要方法为利用频谱仪等硬件设备进行侦测,如图 3 所示,对空间内对应频段的无线信号进行扫描,分析采集信号的带宽和频点等信息,发现异常 RFID 设备的无线信号.此外,文献[21]提出一种利用改进标签(watchdog tag)进行恶意读写器发现的方法.通过改进并增强标签的功能,使其可以解码 RFID 读写器的扫描信息,从而发现恶意读写器的存在.上述两种恶意读写器检测方法的成本较高,应用部署相对复杂,不能对非法设备进行准确检测,如果采用频谱仪进行检测还需关闭正在运行的正常 RFID 设备.此外,检测对象自身物理属性、监控空间电磁环境、人员物品的移动等直接影响了检测的准确度.

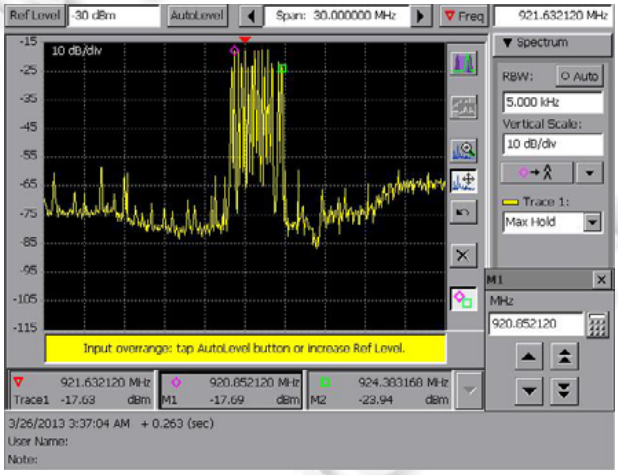

Fig.3 RFID wireless signal detection diagram

图 3 RFID 无线信号检测示意图

综上所述,目前针对 RFID 空中接口数据安全保护的研究已经有了一定的基础,研究内容主要集中在数据加密与安全协议方向.针对 RFID 空口入侵检测的研究主要采用数据分析或额外硬件监测方法加以实现,效率较低且成本偏高,实现难度较大.造成 RFID 空口入侵的根本原因在于恶意读写器的存在,而上述入侵检测方法主要利用数据分析方法发现恶意克隆 RFID 标签,因此对 RFID 空口数据的保护有限.同时,目前针对恶意 RFID 读写器的发现方法主要依靠专业设备进行,操作复杂且成本较高,不利于实际推广应用.

2 RFID 信号传播特征分析

如图 4 所示,正常情况下 RFID 设备的信号传输分为前向数据传输(reader to tag),信号传播模型由 h_f 表示;后向数据传输(tag to reader),信号传播模型由 h_b 表示.

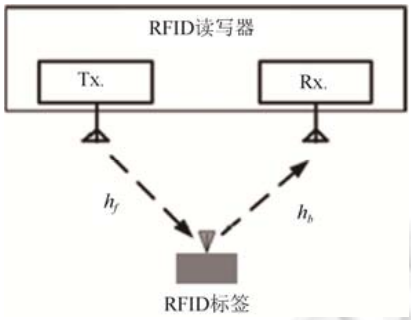

Fig.4 RFID signal transmission diagram

图 4 RFID 信号传播示意图

RFID 系统多部署于室内环境,存在平坦衰落与多径效应,因此反向信号(tag-reader)传播模型与 Rayleigh 模型近似,概率密度函数如公式(1)所示,r 为接收信号包络,σ为 r 被检测前的均方根.

$$h_b = h_{Ray}(r) = \begin{cases} 0, & r < 0 \\ \dfrac{r}{\sigma^2}\exp\exp\left(-\dfrac{r^2}{2\sigma^2}\right), & r \geqslant 0 \end{cases} \tag{1}$$

由于前向信号(reader-tag)传播过程中往往在读写器天线正对方向存在某一主要静态分量,从不同角度随机到达的多径分量迭加在静态分量上,因此,前向传播模型与 Ricean 模型近似,概率密度函数如公式(2)所示,I_0 为 0 阶第 1 类修正贝赛尔函数,a 为主信号分量的幅度峰值.

$$h_f = h_{Ricean}(r) = \begin{cases} 0, & r < 0 \\ \dfrac{r}{\sigma^2}\exp\left(-\dfrac{r^2+a^2}{2\sigma^2}\right)I_0\left(\dfrac{ra}{\sigma^2}\right), & r \geqslant 0, a \geqslant 0 \end{cases} \tag{2}$$

由上述分析可得公式(1)与公式(2),RFID 信号往返传播模型为 $\boldsymbol{h=h_f h_b}$,其概率密度函数如公式(3)所示.

$$p_h(r) = \frac{rexp(-K)}{\sigma_f^2\sigma_b^2}\sum_{i=0}^{\infty}\frac{1}{(i!)^2}\left(\frac{K_\tau}{2\sigma_f\sigma_b}\right)^i K_i\left(\frac{r}{\sigma_f\sigma_b}\right),\ r \geqslant 0 \tag{3}$$

RFID 系统中读写器天线与 RFID 标签位置如图 5 所示,根据电磁波能量传播原理,标签接收的信号功率 $P_{r,T}$ 如公式(4)所示[22].

$$P_{r,T} = \rho_L P_{Tx} G_T G_R(d,H,\theta,\phi) PL(d) {h_f}^2 \tag{4}$$

如果标签接收的信号功率满足工作条件,则读写器天线接收到的反向散射信号功率 $P_{r,R}$ 如公式(5)所示.

$$P_{r,R} = \tau\mu_T\rho_L P_{Tx}\left|G_T G_R PL(d)\right|^2\left|h_f\right|^2\left|\Gamma\right|^2\left|h_b\right|^2 \tag{5}$$

因此,RFID 系统可以正常工作的条件为天线接收的标签反射功率大于天线所要求的最低功率阈值($P_{r,R} \geqslant P_{RS}$),即系统正常工作的概率为 P_D=1–P_r,根据已知概率密度公式可得系统正常工作概率 P_D 如公式(6)所示,其中,A_{th} 为最低工作功率对应的信号包络大小.

$$P_D(P_{RS}) = 1 - \int_0^{A_{th}} p_h(r)\mathrm{d}r \tag{6}$$

对公式(6)的内容进行仿真计算,结果如图 6 所示.其中,图 6(a)所示为 Rice 系数 K=100,即自由空间条件下标签在平面内各位置时 RFID 系统正常工作的概率,图 6(b)所示为 Rice 系数 K=1 时,即存在外界干扰时标签在平

面内各位置时 RFID 系统正常工作的概率.

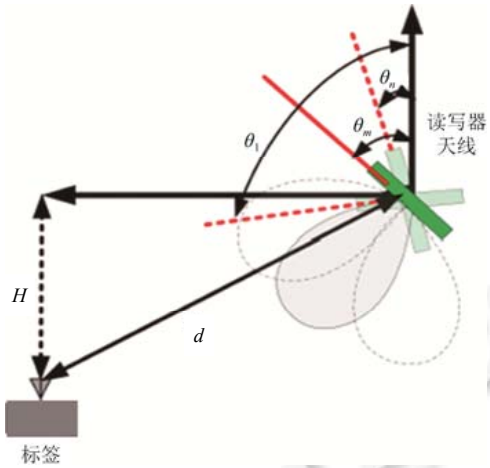

Fig.5 Communication between reader and tag

图 5 读写器与标签通信示意图

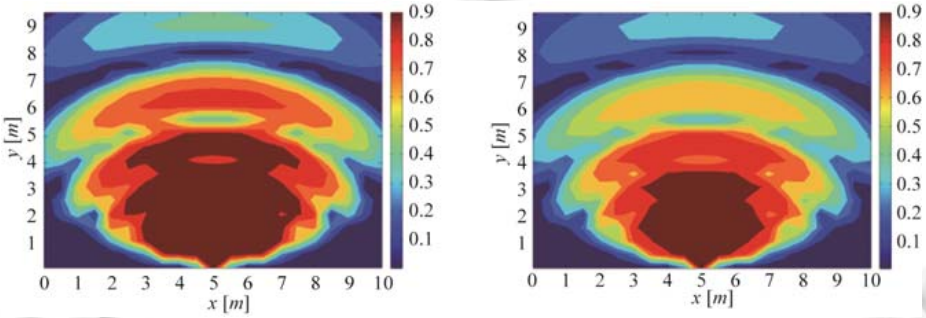

Fig.6 The probability of reader correctly acquires the data

图 6 读写器正常获取数据概率示意图

根据仿真结果可得,空间中不同距离、不同角度位置下读写器成功获取数据的概率存在差异.

3 恶意 RFID 读写器干扰分析

3.1 恶意RFID读写器干扰类型

RFID 系统采用后向散射传输方式,标签获取的驱动能量和反射的后向传输能量均较为微弱,容易受到外界 RFID 设备的干扰,因此可以通过合法 RFID 信号受到干扰的情况来判别是否存在恶意读写器.如图 7 所示,已知的恶意读写器对 RFID 系统的干扰分为两种:R→T(读写器→标签)干扰和 R→R(读写器→读写器)干扰.

R→T 干扰:当恶意读写器与已部署读写器同时读取同一个标签时,会引发读写器到标签之间的干扰.两个读写器的读取范围出现重叠,恶意读写器 R1 与合法读写器 R2 发射的信号可能在射频标签 T1 处产生碰撞.在这种情况下,标签 T1 与合法读写器 R2 的通信被干扰,无线信道状态参数受到影响.

R→R 干扰:读写器之间的干扰是指:恶意读写器发射的较强的信号与标签反射给合法读写器的微弱信号产生干扰,引起读写器与读写器之间的干扰.合法读写器 R1 位于恶意读写器 R2 的工作范围内,标签 T1 在 R1 的覆盖范围内.当标签 T1 反射回的微弱信号传输给读写器 R1 的过程中,很容易被恶意读写器 R2 发射的强信号干扰.R1 很难读取到 T1 返回的正确信号.

UHF 频段内较为常用的 RFID 通信的标准是 EPC C1 G2,该标准同时被 ISO 18000-6C 采纳.在该标准下 RFID 系统存在两种工作模式:一种是多 RFID 读写器模式,在特定的空间区域内处于工作状态的读写器数量少于通信信道的数量;另一种是密集 RFID 读写器模式,在特定的空间区域内处于工作状态的读写器数量多于或等于通信信道的数量.EPC C1G2 对 RFID 通信信道和频段进行了严格划分,如图 8 所示.

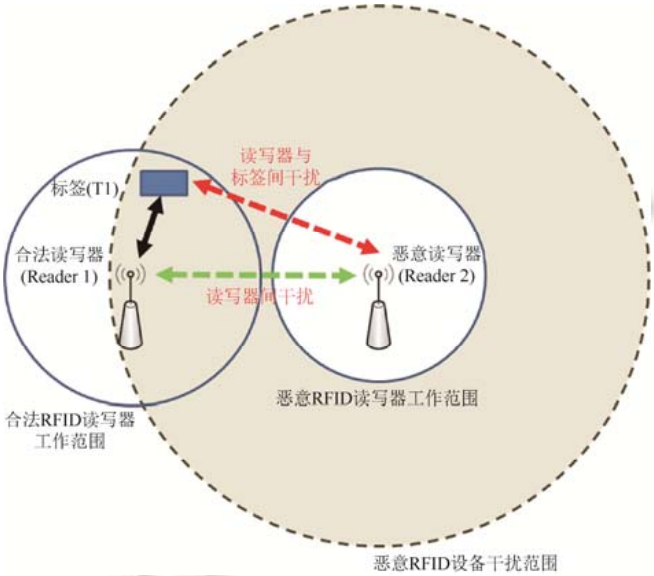

Fig.7 Malicious reader interference diagram

图 7 恶意读写器干扰示意图

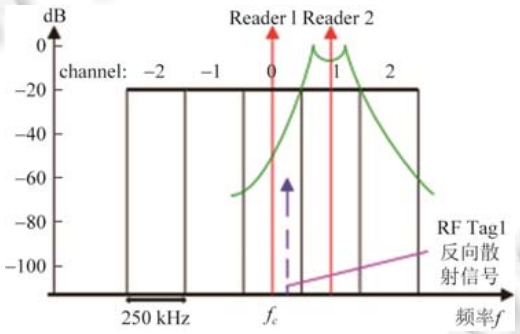

Fig.8 Channel division and adjacent channel interference

图 8 信道划分及临近信道干扰

在多读写器工作模式下,由于 RFID 读写器在不同的工作信道间调频工作,因此恶意读写器会对已部署的 RFID 系统产生 R→T 和 R→R 两种干扰,影响无线信号状态.在密集读写器工作模式下,RFID 系统中读写器到标签的通信在奇数信道进行,即 1、3、5 等信道,标签至读写器通信在偶数信道,即 2、4、6 等信道进行.由于前向通信和后向通信各自占用不同的信道,所以根据此标准可避免恶意读写器对标签信号的干扰,但由于标签无法对信道进行判断,因此恶意读写器仍然会对合法 RFID 设备产生干扰,影响 RFID 信号.

3.2 恶意RFID读写器干扰影响分析

由恶意读写器存在时产生的两种信号干扰可知,如果存在恶意读写器,则会降低合法读写器工作范围内每个位置上成功获取数据的概率.定义信号-干扰噪声比 SIR 如式(7)所示,N 为环境噪声,I 为干扰信号强度大小.

$$SIR_{(d)}=\frac{P_{r,R}(d)}{N+\sum_i I(i)} \tag{7}$$

根据文献[23]对公式(6)进行修改,得到在恶意读写器存在情况下成功获取数据的概率分布如公式(8)所示,其中,K_0 为合法设备莱斯系数,K_I 为非法设备莱斯系数,N 为非法设备数量,Q 为 Marcum 函数.

$$\left.\begin{aligned}D_I\left(K_0,K_I,N_I,\mathrm{SIR}_{th}\right)=1-Q\left(\sqrt{\frac{2K_IN_I\mathrm{SIR}_{th}}{b_1+\mathrm{SIR}_{th}}};\sqrt{\frac{2K_0b_1}{b_1+\mathrm{SIR}_{th}}}\right)+\exp\left(-\frac{K_IN_I\mathrm{SIR}_{th}+K_0b_1}{b_1+\mathrm{SIR}_{th}}\right)\times\\ \sum_{n=0}^{N_I-1}\left(\frac{K_0\mathrm{SIR}_{th}}{K_IN_Ib_1}\right)^{\frac{n}{2}}I_n\left(\sqrt{\frac{4N_IK_0K_Ib_1\mathrm{SIR}_{th}}{b_1+\mathrm{SIR}_{th}}}\right)\times\left\{\left(1+\frac{b_1}{\mathrm{SIR}_{th}}\right)^{-N_1}\sum_{k=n}^{N_I-1}\binom{N_I}{k-n}\left(\frac{b_1}{\mathrm{SIR}_{th}}\right)^k-\delta_{n0}\right\}\end{aligned}\right\} \tag{8}$$

恶意读写器存在与消失两种情况下的概率分布结果如图 9 所示,分析模拟仿真计算的结果可得,存在非法设备情况下读取概率下降异常迅速,从而得出以下两点推论.

(1) 相同读取概率情况下,存在恶意读写器将缩短原有 RFID 系统的有效工作距离,缩小合法读写器读取范围;

(2) 相同读取距离情况下,存在恶意读写器将降低原有 RFID 系统的读取概率,进而降低标签的读取速率.

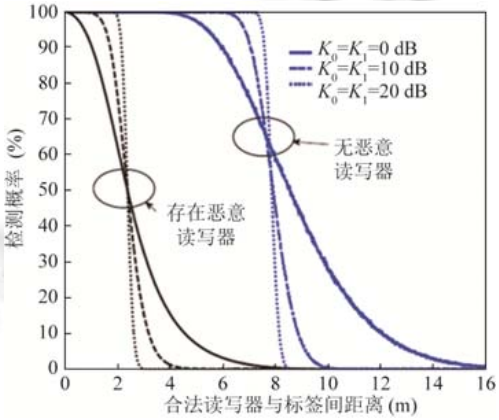

Fig.9 Simulation of malicious reader's effect

图 9 恶意读写器影响结果仿真计算图

4 恶意 RFID 读写器判别模型设计

4.1 判别模型作用范围分析

为建立判别模型,首先需要通过计算确立判别模型的有效作用范围.如图 10 所示,考虑读写器间干扰情况,判别模型的有效作用条件为合法读写器位于恶意读写器的干扰范围之内;考虑读写器标签间干扰情况,设恶意 RFID 读写器与标签的距离为 d_I,合法 RFID 读写器与标签的距离为 d_R.如公式(9)所示,根据 Cole 提出的损耗模型计算判别模型的有效作用范围.

$$PathLoss=\begin{cases}32+25\log(d), & \text{if } \lambda\leqslant d\leqslant d_m\\ 23+35\log(d), & \text{if } d\geqslant d_m\end{cases} \tag{9}$$

公式(9)中,$PathLoss$ 为信号衰减,λ为射频信号的波长,d_m 是近场和远场的分界值,超高频 RFID 一般工作在远场区,即 $d>d_m$.如果恶意读写器对标签不产生干扰,则无法对其进行检测,因此判别模型作用范围即为恶意读写器对标签的最大干扰距离.已知当读写器与标签通信时,如果发送到标签处的信号强度超过干扰信号强度 13dB,则标签可以不受干扰信号的影响.设恶意读写器与合法读写器的发射功率为 P,可得判别模型作用范围为

$$P-(23+35\log d_R)-(P-(23+35\log d_I))>13 \tag{10}$$

解得 $\frac{d_I}{d_R}$>2.35.

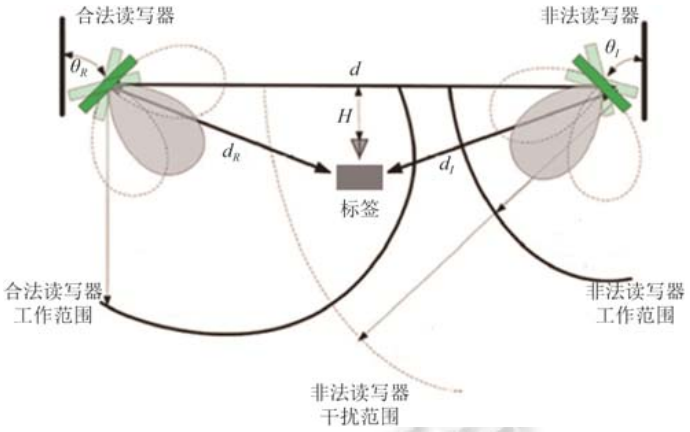

Fig.10 The interference effect of RFID system

图 10 RFID 系统干扰效应示意

综上所述,若恶意读写器与标签的距离小于正常读写器与标签距离的 2.35 倍,则判别模型有效.

4.2 恶意读写器判别模型建立

根据图 8 所得两点推论,利用合法读写器读取范围减少比率 IRRR(interrogation range reduction ratio)和合法读写器读取速度减少比率 DRRR(detection rate reduction ratio)可以有效反映空间中恶意读写器的存在情况. IRRR 的定义如公式(11)所示,$Range_{\max}$ 为参考标签与合法读写器角度 θ、高度 H 情况下的最大识读距离; $Range_{\mathrm{Mal}}$ 为存在恶意读写器情况下的最大识读距离.

$$IRRR_{(\theta,H)}=\frac{Range_{\max}-Range_{\mathrm{Mal}}}{Range_{\max}} \tag{11}$$

DRRR 的定义如公式(12)所示,$Rate_{\max}$ 为在参考标签与合法读写器角度为 θ、高度为 H 情况下的最大读取速率,$Rate_{\mathrm{Mal}}$ 为存在恶意读写器情况下的最大读取速率.

$$DRRR_{(\theta,H)}=\frac{Rate_{\max}-Rate_{\mathrm{Mal}}}{Rate_{\max}} \tag{12}$$

本研究根据已经确定的信号传播模型,推导出 IRRR、DRRR 在存在恶意读写器情况下的变化情况,并与实际测试数据相比进行验证,计算得出无线信号度量参数(MRDP)及其置信区间,利用度量参数 MRDP 建立恶意 RFID 读写器判别模型.

如公式(13)所示,判别模型采用多元回归方法,计算环境中恶意读写器与合法读写器在不同距离(d)、不同角度(θ)、不同速度(v)、不同高度(H)等情况下对度量参数 MRDP 的影响程度.

$$MRDP=\beta_1+\beta_2 d_i+\beta_3\theta_i+\beta_4 v_i+\beta_5 H_i+\mu_i \tag{13}$$

在多元回归方法的基础上,计算回归系数 $\beta=\beta_1+\beta_2+\beta_3+\beta_4+\beta_5$, 进而建立基于度量参数的恶意读写器判别模型.

5 判别模型度量参数获取

根据本文第 4.2 节所得结论,读写器的识读距离和读写速率作为指标对恶意读写器的入侵会有较好的反馈.在判别模型实际建立过程中,我们使用 RFID 标签的吞吐率作为度量参数 $MRDP$ 的表示指标.吞吐率 N 的计算公式如下,其中,n 表示 RFID 读写器读取的标签总次数,t 表示读取时间.

$$N=\frac{n}{t} \tag{14}$$

在遭到恶意读写器入侵干扰时,合法读写器的最大识读距离将会减小,原来识读范围内的标签可能无法再读到.同时,最大读写速度由于信道冲突干扰等等,也会随之减小.反应在吞吐量上,都会带来吞吐量明显的改变.此外,可以作为 *MRDP* 度量参数的指标还有信号强度 *RSSI* 等指标.为确定判别模型采用度量参数的最终指标,本研究分别对各个指标进行实验测试与验证.

通过测试在恶意读写器 *B* 存在的情况下,合法读写器 *A* 接收到的信号强度、吞吐量与距离以及角度之间的结果,由公式(10)可得,当恶意读写器 *B* 与标签的距离小于正常读写器与标签距离的 2.35 倍时,才会对合法读写器 *A* 采集的信号结果产生干扰,所以,恶意读写器的位置(角度和距离)需满足上述原则.

如图 11 所示,本次测试选择在 RFID 读写器正面 30°~120°范围内进行.测试距离为近(20cm)、中(60cm)、中远(110cm)、远(180cm)这 4 个相对位置.

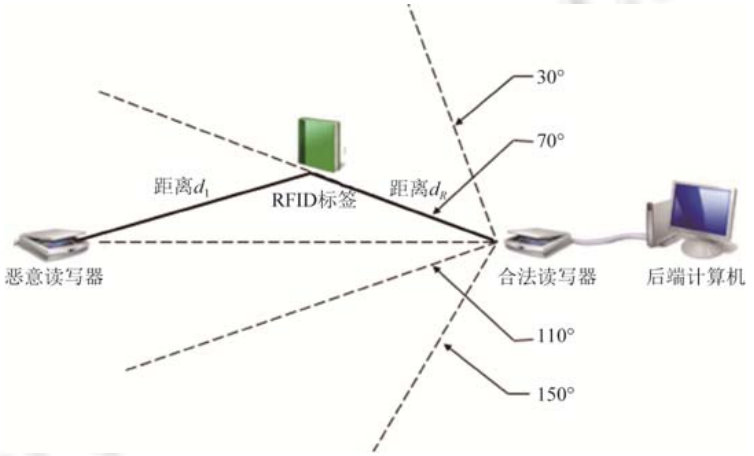

Fig.11 Deployment of experimental environment

图 11 部署实验环境示意图

测试数据见表 1.由数据可得,恶意读写器 *B* 出现之后,读写器 *A* 的信号强度(RSSI)和相位变化范围较小,但吞吐率会下降得非常明显,因此,吞吐率最适合度量参数 *MDRP* 的表示指标来反映恶意读写器的存在情况.

Table 1 Comparison between double reader *A*, *B* and single reader *A* data

表 1 双读写器 *A*,*B* 与单读写器 *A* 测量数据对比

方向	距离/cm	入侵前后	RSSI/dB	吞吐率/s	方向	距离/cm	入侵前后	RSSI/dB	吞吐率/s
30°	20	前	–47.5	24.21	110°	20	前	–44.4	24.2
30°	20	后	–47.5	13.01	110°	20	后	–44.4	9.875
30°	60	前	–49.8	24.26	110°	60	前	–58.6	21
30°	60	后	–50	8.1	110°	60	后	–58.6	8.82
30°	110	前	–56.5	24.5	110°	110	前	–54.2	25.31
30°	110	后	–56.1	3.79	110°	110	后	–54	3.05
30°	180	前	–55.8	18.02	110°	180	前	–56.6	23.232
30°	180	后	–55.5	5.32	110°	180	后	–57.5	0.577
70°	20	前	–45.2	24.38	150°	20	前	–40.5	24.16
70°	20	后	–45.3	10.18	150°	20	后	–40.6	13.11
70°	60	前	–48.4	22.9	150°	60	前	–45.9	26
70°	60	后	–48.9	10.588	150°	60	后	–45.7	10.5
70°	110	前	–51.3	22.31	150°	110	前	–54.5	22.13
70°	110	后	–50.8	11.714	150°	110	后	–54.2	4.14
70°	180	前	–54.5	25.22	150°	180	前	–54.2	18.3
70°	180	后	–54.3	8.77	150°	180	后	–54.2	6.82

6 基于有限状态机的判别模型实现

6.1 异常度量参数实时动态监测方法

有限状态机是表示有限个状态以及在这些状态之间的转移和动作等行为的数学模型,利用有限状态机模型可以很好地进行度量参数变化的判断,实现对异常感知数据的识别,因此,本研究基于有限状态机模型,完成异常度量参数的动态检测,实现恶意读写器的发现感知.如图 12 所示,有限状态机模型由五元组构成,记作 $M=(S,\Sigma,f,S_0,Z)$.

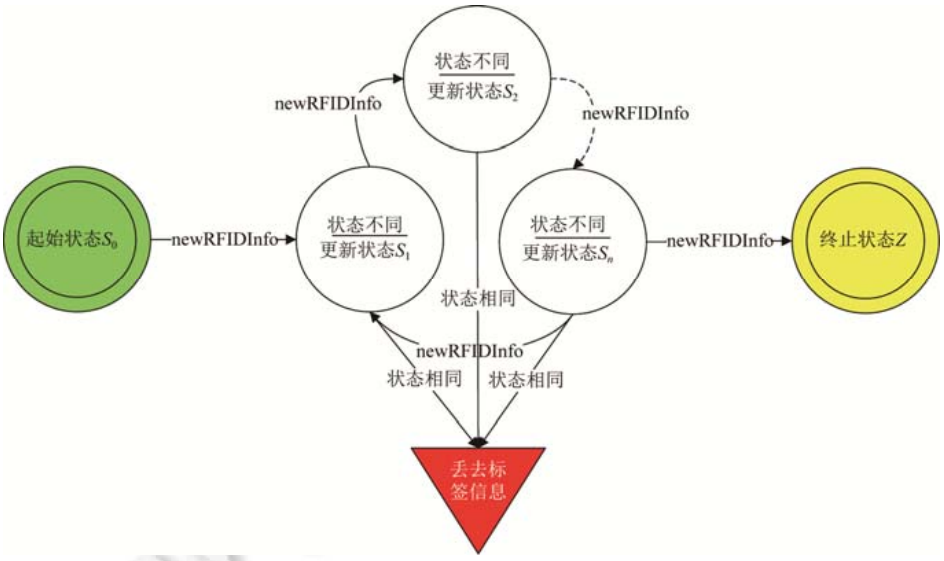

Fig.12 A model of inference model for finite state machine

图 12 有限状态机的推断模型示意图

$S=\{\text{状态}i\}$, S 是一个有限集,其中,每一个元素代表每一时刻的 RFID 信号度量参数.状态集可以反映当前时刻室内环境中恶意读写器对于度量参数的影响,刻画出当前室内环境中的状态.

$\Sigma=\{\text{输入字符}i\}$, Σ是一个有穷字母表,它的每一个元素称为一个输入字符,在模型建立过程中,输入字符为环境中不同的变化因素.其中,每一条信息都包含环境、位置与时间的状态信息.

$f:S\times\Sigma\Rightarrow S$ 是状态转换函数,表示某状态接受某个新输入字符后所转变的状态;在该实验场景中,状态转移函数表示为:如果当前状态与下一时刻输入的度量参数处于正常区间以外,那么状态集 S 改变为下一时刻状态,否则状态集 S 保存原有状态.

$S_0\in S$, S_0 是 S 中的一个元素,是 RFID 信号度量参数的初始状态;在实验环境条件下,S_0 表示:系统给予室内环境设定的初始状态.

$Z\subseteq S$, 且 $Z\neq\varnothing$, Z 是 S 的一个子集,是有限状态机的终止状态集.在实验环境中,Z 表示度量参数最后一次改变后的状态[24].

根据有限状态机理论,检测方法需要记录被监控环境中各个时刻度量参数的信息,推断模型将当前度量参数状态 S_0 与上一时刻度量参数状态 S_1 进行比较,进入状态 S_2,根据建立的判别模型中度量参数的变化范围和置信区间进行判断,如果度量参数正常,即室内环境未发生变化,无恶意读写器存在,返回状态 S_1;如果独立参数异常,即室内环境变化,存在恶意读写器,系统更新状态信息进入 S_3,进行报警操作后再返回状态 S_1,以此完成恶意读写器实时发现,实现 RFID 空口入侵检测.

6.2 度量参数置信区间计算与判别模型实现

根据有限状态机模型,首先计算稳态吞吐率 *N_standard*,作为后续判断有无读写器入侵的标准.由于系统的

工作环境复杂多样,因此,使用人工实验测试计算稳态值,效率低且不具备比较意义.因此,本研究提出自适应计算稳态的算法,在恶意读写器监控系统工作前先进行数据收集,计算出吞吐率的初始平均值,并将其作为监控系统开始工作后的判别依据.在环境参数改变时,重置计算,再次收集数据生成稳态便可适应新环境.

其次,根据计算的初始值,利用相对误差的计算方法,本研究引入变化量相对差概念作为是否存在恶意读写器的判断依据.设每段周期时间计算出的吞吐率为 N,相对差为 G.测试数据见表 2.

$$G=\frac{|N-N\_standard|}{N\_standard} \tag{15}$$

Table 2 Changes of throughput before and after the invasion about different distance, angle

表 2 不同距离、角度入侵前后吞吐量变化情况

距离角度(cm)	信号强度与吞吐量相对差									
	90°		270°		0°		45°		315°	
20	–44.4	0.480 1	–40.5	0.492 5	–47.5	0.461 5	–45.2	0.405 2	–44.3	0.472 2
60	–58.6	0.580 0	–49.9	0.666 1	–45.8	0.596 2	–48.6	0.537 6	–51.2	0.477 2
110	–54.1	0.879 5	–54.4	0.812 9	–56.4	0.845 3	–51.1	0.474 9	–58.8	0.718 9
180	–57.0	0.975 2	–54.2	0.627 3	–55.6	0.704 8	–54.4	0.652 3	–55.7	0.610 0

根据表 1 中的数据可得,信号强度-距离-吞吐率相对差三者有一定相关性,我们以吞吐率作为度量参数 *MRDP* 的主要判别指标,利用此相关性,计算判别模型的度量参数的判断条件及其置信区间.对信号强度与吞吐率相对差的关系使用最小二乘法进行一元多项式拟合($G=a_0x_2+a_1x+a_2$),得到的系数为 a_0=0.000428,a_1=0.02287,a_3=0.6582.因此,根据计算结果,将 $G>(G_ploy-0.2776)$作为判定模型中恶意读写器是否出现的判断条件,其中,当相对差预测值 G_ploy 显著性为 0.95 时,置信区间为 0.277 6.

7 实验测试与验证

为验证本文提出的恶意读写器判别模型及其实现方法的有效性与实时性,我们利用通用 RFID 读写设备进行了测试验证实验.实验采用 UHF 频段的 Impinj R420 读写器和标签作为测试对象,测试环境如图 13 所示.合法 RFID 读写器天线位置固定,将合法 RFID 读写器通过网线与已经部署判别模型程序的计算机相连接,在合法 RFID 读写器天线正面随机选取 10 个 RFID 标签测试位置进行实验,每个 RFID 标签位置进行 100 次模拟恶意读写器入侵实验.当合法 RFID 读写器与标签正常通信开始工作后,利用另一台同样型号的 RFID 读写器模拟恶意读写器随机进入合法读写器工作范围,根据计算机判别模型程序计算结果给出最后检测结论.

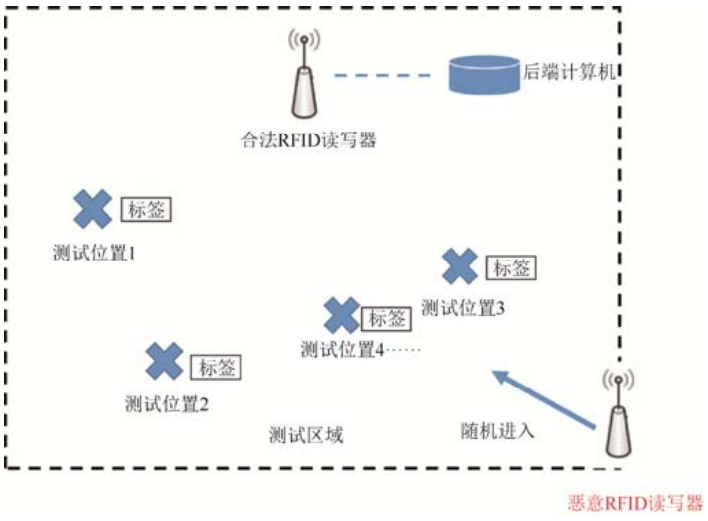

Fig.13 Test field map

图 13 测试场地示意图

(1) 开阔场地单标签工作情况

测试场地较为开阔,标签与读写器之间无障碍物,合法读写器工作范围内每个 RFID 标签位置测试时放置一个 RFID 标签.系统启动开始数据采集,设置自适应算法的计算时间为 5s,计算出单个标签的吞吐率初始平均值,作为判断阈值.随后,恶意 RFID 读写器从随机位置进入测试区域,记录标签吞吐率变化情况,利用检测算法判

断是否存在恶意读写器,记录本次检测结果,每个位置共进行 100 次测试,测试结果见表 3.判别模型程序识别准确率为 97.3%,平均检测时间为 1.58s.

(2) 开阔场地多标签工作情况

测试场地较为开阔,标签与读写器之间无障碍物,合法读写器工作范围内每个 RFID 标签位置测试时放置多个 RFID 标签,系统启动开始数据采集,设置自适应算法的计算时间为 5s,计算出多个标签的吞吐率初始平均值,作为判断阈值.随后,恶意 RFID 读写器从随机位置进入测试区域,记录标签吞吐率变化情况,利用检测算法判断是否存在恶意读写器,记录本次检测结果,每个位置共进行 100 次测试,测试结果见表 4.判别模型程序识别准确率为 95.7%,平均检测时间为 1.72s.

Table 3 Test result form for scene 1

表 3 情景 1 测试结果统计表

标签位置	位置 1	位置 2	位置 3	位置 4	位置 5	位置 6	位置 7	位置 8	位置 9	位置 10
发现次数	96	98	98	98	96	97	98	97	98	97
平均检测时间(s)	1.35	2.17	1.89	1.54	2.11	1.21	1.04	1.44	1.21	1.87

Table 4 Test result form for scene 2

表 4 情景 2 测试结果统计表

标签位置	位置 1	位置 2	位置 3	位置 4	位置 5	位置 6	位置 7	位置 8	位置 9	位置 10
发现次数	94	95	98	95	94	97	98	95	95	96
平均检测时间(s)	2.11	1.45	1.43	1.59	1.43	1.98	1.78	2.22	2.41	1.22

(3) 复杂场地单标签工作情况

测试场地内存在各类干扰,标签与读写器之间障碍物随机分布,合法读写器工作范围内每个 RFID 标签位置测试时放置一个 RFID 标签,系统启动开始数据采集,设置自适应算法的计算时间为 5s,计算出单个标签的吞吐率初始平均值,作为判断阈值.随后,恶意 RFID 读写器从随机位置进入测试区域,记录标签吞吐率变化情况,利用检测算法判断是否存在恶意读写器,记录本次检测结果,每个位置共进行 100 次测试,测试结果见表 5.判别模型程序识别准确率为 95.3%,平均检测时间为 1.75s.

Table 5 Test result form for scene 3

表 5 情景 3 测试结果统计表

标签位置	位置 1	位置 2	位置 3	位置 4	位置 5	位置 6	位置 7	位置 8	位置 9	位置 10
发现次数	95	95	97	92	94	94	96	98	95	97
平均检测时间(s)	1.45	1.68	1.73	1.88	2.34	2.15	1.08	1.78	1.85	1.54

(4) 复杂场地多标签工作情况

测试场地内存在各类干扰,标签与读写器之间障碍物随机分布,合法读写器工作范围内每个 RFID 标签位置测试时放置多个 RFID 标签,系统启动开始数据采集,设置自适应算法的计算时间为 5s,计算出多个标签的吞吐率初始平均值,作为判断阈值.随后,恶意 RFID 读写器从随机位置进入测试区域,记录标签吞吐率变化情况,利用检测算法判断是否存在恶意读写器,记录本次检测结果,每个位置共进行 100 次测试,测试结果见表 6.判别模型程序识别准确率为 95.2%,平均检测时间为 1.78s.

Table 6 Test result form for scene 4

表 6 情景 4 测试结果统计表

标签位置	位置 1	位置 2	位置 3	位置 4	位置 5	位置 6	位置 7	位置 8	位置 9	位置 10
发现次数	95	96	94	94	97	93	95	96	95	97
平均检测时间(s)	2.17	1.65	1.78	1.89	1.65	1.47	1.87	1.29	1.97	2.08

综上所述,不同场景下本文提出的判别模型计算准确度均高于 95%,且平均检测时间不超过 1.8s,判别算法准确性较高,实时性较强,且不依赖于外部设备,检测方法成本较低,对发现恶意 RFID 读写器、保护 RFID 系统的空口数据安全具有较高的实际应用价值.

8 结 论

针对 RFID 系统中存在的空口数据入侵这一安全威胁,本文通过恶意 RFID 读写器对正常工作 RFID 系统无线信号产生影响这一现象进行系统的研究与分析,提出了基于吞吐率相对差为指标的 RFID 信号度量参数,利用度量参数快速、准确感知环境中 RFID 信号的变化情况.在此基础上,基于多元回归方法建立恶意 RFID 读写器判别模型,计算恶意 RFID 读写器的判别条件与置信区间.利用有限状态机模型实现异常度量参数的快速动态检测,实时发现空间中存在的恶意读写器,保证了对 RFID 空中接口入侵检测的实时性与有效性,减少 RFID 系统中因空口数据被窃取产生的安全威胁,提高 RFID 技术应用的安全性和可靠性,保障系统数据的隐私性.

本研究充分利用已广泛部署的 RFID 设备,根据 RFID 信号参数的变化进行实时分析,实现恶意读写器的准确、快速发现.本方法主要针对室内环境中的无源 UHF 频段 RFID 通用设备,相比于其他 RFID 空口入侵检测方法,本方法利用 RFID 系统自身的硬件与数据,不依赖附加的检测设备与工具,降低了 RFID 空口入侵检测的复杂程度与应用成本,易于在实际环境中广泛部署应用.同时,由于采用了自适应算法计算不同环境的状态阈值,本方法可以很好地适用不同的室内环境.下一步我们将进一步完善本方法的实际部署方案和应用模式,提高自适应算法的计算效率,使得检测模型可以在不同的室内环境中快速部署应用.

References:

[1] Werb J, Lanz1 C. Designing a positioning system for finding things and people indoors. IEEE Spectrum, 1998,35(9):71−78.

[2] Tan M, Liu Y, Zeng JF. RFID Technical System Engineering and Application Guide. Beijing: Mechanical Industry Publishing House, 2007. 32−53 (in Chinese).

[3] Jari-Pascal C, Wrote; Chen LY, Mao LH, ed. Design and Optimization of Passive UHF RFID System. Beijing: Science Press, 2008. 31−52 (in Chinese).

[4] Information technology—Radio frequency identification—Air interface protocol at 800/900 MHz.2013 (in Chinese).

[5] Information technology—Radio frequency identification—Air interface protocol at 2.45 GHz.2012 (in Chinese).

[6] Air interface for military radio frequency identification part 1:800/900 MHz.2011 (in Chinese).

[7] Juels A. Minimalist cryptography for low-cost RFID tags. In: Security in Communication Networks. LNCS 3352, 2005. 149−164.

[8] Feldhofer M, Dominikus S, Wolkerstorfer J. Strong authentication for RFID systems using the AES algorithm. LNCS, 2004, 3156:357−370.

[9] Golle P, Jakobsson M, Juels A, Syverson P. Universal re-encryption for mixnets. LNCS, 2004,2964:163−178.

[10] Saito J, Ryou JC, Sakurai K. Enhancing privacy of universal re-encryption scheme for RFID tags. LNCS, 2004,3207:879−890.

[11] Li JC. Research and implementation technologies of communication protocol for RFID air interface [Ph.D. Thesis]. Changsha: National University of Defense Technology, 2011 (in Chinese with English abstract).

[12] Jia QX, Chen P, Gao X, Wei LY, Wang X, Zhao B. Lightweight anti-desynchronization RFID mutual authentication protocol. Journal of Central South University (Science and Technology), 2015,6:2149−2156 (in Chinese with English abstract).

[13] Pang LJ, He L, Pei Q, Wang Y. Secure and efficient mutual authentication protocol for RFID conforming to the EPC C-1 G-2 Standard. In: Proc. of the 2013 IEEE Wireless Communications and Networking Conf. IEEE Computer Society, 2013. 1870–1875.

[14] Good N, Han J, Miles E, Molnar D, Mulligan D, Quilter L, Urban J, Wagner D. Radio frequency identification and privacy with information goods. In: Proc. of the Workshop on Privacy in the Electronic Society—WPES. 2004. 41–42.

[15] Zhang R, Zhu LH, Xu C, Yi Y. An efficient and secure RFID batch authentication protocol with group tags ownership transfer. In: Proc. of the IEEE Conf. on Collaboration and Internet Computing. 2015. 168–175.

[16] Sridhar GTR. Intrusion detection in RFID systems. Military Communications Conf., 2008,20(1):1–7.

[17] Razm A, Alavi SE. An intrusion detection approach using fuzzy logic for RFID system. In: Advances in Information Science and Applications-Volume II. 2014.

[18] Darcy P, Stantic B, Mitrokotsa A, Sattar A. Detecting intrusions within RFID systems through non-monotonic reasoning cleaning. In: Proc. of the Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP). 2010.

[19] Guo JH, Yang HD, Deng FQ. Intrusion detection model for RFID system based on immune network. Journal of Computer Applications, 2008,28(10):2481−2484 (in Chinese with English abstract).

[20] Metzger C, Florkemeier C, Bourquin P. Making radio frequency identification visible—A watchdog tag. In: Proc. of the Pervasive Computing and Communications Workshops. New York: IEEE, 2007. 352−356.

[21] Bekkali A, Zou S, Kadri A, Penty R. Impact of reader-to-tag interference and forward link fading on RFID system performance. In: Proc. of the IEEE WCNC. 2014.

[22] Tjhung TT, Chai CC, Dong X. Outage probability for lognormal-shadowed Rician channels. IEEE Trans. on Vehicular Technology, 1997,46:400–407.

[23] Luo YJ, Jiang JG, Wang SY, Jing X, Ding C, Zhang ZJ, Zhang YF. Filtering and cleaning for RFID streaming data technology based on finite state machine. Ruan Jian Xue Bao/Journal of Software, 2014,25(8):1713–1728 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4666.htm [doi: 10.13328/j.cnki.jos.004666]

附中文参考文献:

[2] 谭民,刘禹,曾隽芳.RFID 技术系统工程及应用指南.北京:机械工业出版社,2007.32–53.

[3] Jari-Pascal C 著;陈力颖,毛陆虹,译.无源超高频 RFID 系统设计与优化.北京:科学出版社,2008.31−52.

[4] GB/T 29768-2013.信息技术射频识别 800/900MHz 空中接口协议.2013.

[5] GB/T 28925-2012.信息技术射频识别 2.45GHz 空中接口协议.2012.

[6] GJB 7377.1-2011.军用射频识别空中接口协议(第 1 部分):800/900MHz 参数.2011.

[11] 李建成.射频识别系统空中接口通信协议关键技术研究与实现[博士学位论文].长沙:国防科技大学,2011.

[12] 贾庆轩,陈鹏,高欣,韦凌云,王鑫,赵兵.抗去同步化的轻量级 RFID 双向认证协议.中南大学学报(自然科学版),2015,6:2149–2156.

[19] 郭建华,杨海东,邓飞其.基于免疫网络的 RFID 入侵检测模型研究.计算机应用,2008,28(10):2481–2484.

[23] 罗元剑,姜建国,王思叶,景翔,丁昶,张珠君,张艳芳.基于有限状态机的 RFID 流数据过滤与清理技术.软件学报,2014,25(8):1713–1728. http://www.jos.org.cn/1000-9825/4666.htm [doi: 10.13328/j.cnki.jos.004666]

黄伟庆(1972－),男,北京人,正高级工程师,博士生导师,CCF 高级会员,主要研究领域为物联网安全,空间电磁信号发射机理,通信与异常信号盲均衡处理,微弱信号提取,未知信号调制模式识别与参数估计.

丁昶(1990－),男,博士生,CCF 专业会员,主要研究领域为物联网,信息安全.

崔越(1994－),男,博士生,主要研究领域为信息安全.

王思叶(1981－),女,高级工程师,CCF 专业会员,主要研究领域为物联网,信息安全.

张艳芳(1987－),女,工程师,主要研究领域为物联网,信息安全.

赵博白(1993－),男,博士生,主要研究领域为物联网,数据融合.

诸邵忆(1994－),女,博士生,主要研究领域为物联网,隐私保护.

毛锐(1982－),女,高级工程师,主要研究领域为网络安全.

陈超(1985－),女,工程师,主要研究领域为信息安全.