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.

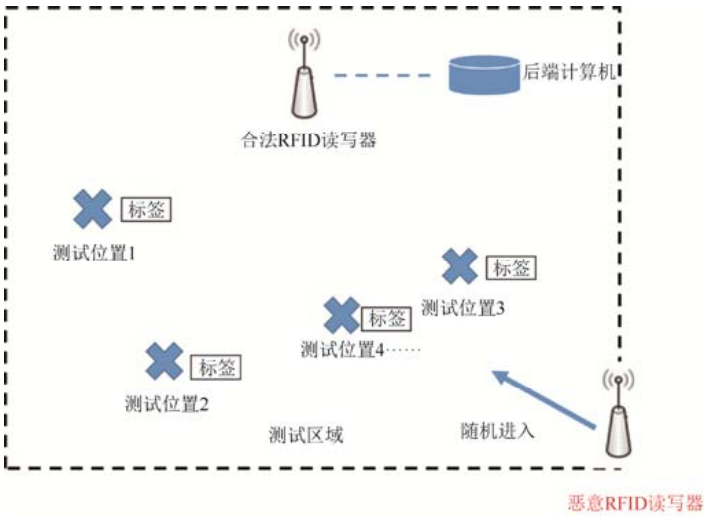


Fig.13 Test field map

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.