

基于标签分组的新型 Q 值防碰撞算法

杨子薇 郑嘉利 岳世彬 袁源 石静

(广西大学计算机与电子信息学院 南宁 530004) (广西多媒体通信与网络技术重点实验室 南宁 530004)

摘要 RFID 技术是物联网的关键技术,为了解决射频识别技术中大量标签数据的防碰撞问题,提出了一种基于 EPC-C1G2 标准的 Q 值算法。该算法对原 Q 值算法中 Q 的取值方法进行了有效改进,同时结合标签分组算法,解决了在大量标签数据的情况下,如何保持较高的系统效率的问题。仿真结果表明,与传统算法相比,提出的改进算法不仅能够减少时隙数,提高时隙利用率,而且可以维持较好的系统吞吐率。

关键词 RFID, EPC-C1G2, Q 值算法, 标签分组

中图分类号 TP391, TN92 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.09.024

New Q Value Anti-collision Algorithm Based on Label Grouping

YANG Zi-wei ZHENG Jia-li YUE Shi-bin YUAN Yuan SHI Jing

(School of Computer and Electronic Information, Guangxi University, Nanning 530004, China)

(Guangxi Key Laboratory of Multimedia Communications and Network Technology, Nanning 530004, China)

Abstract RFID technology is a key technology of the Internet of things. In order to solve the problem of anti-collision in RFID technology with a large number of tag data, a new Q value algorithm based on EPC-C1G2 was proposed in this paper. In this algorithm, the method of Q is improved effectively. Otherwise, combined with the label grouping algorithm, the proposed method achieves higher system efficiency in a large number of tag data. The simulation results show that the proposed algorithm can not only reduce the slot number, improve the time slot utilization, but also maintain a good system throughput rate.

Keywords RFID, EPC-C1G2, Q algorithm, Label grouping

1 引言

物联网是在互联网的基础上,将其用户端延伸和扩展到任何物品,进行信息交换和通信的一种网络。物联网的关键技术——射频识别(Radio Frequency Identification, RFID)技术是一种通过射频信号进行非接触式识别的自动识别技术,可对被识别物体进行识别^[1]。在多个阅读器和多个标签的 RFID 系统中,存在着两种形式的冲突方式:1)同一标签同时收到不同阅读器发出的命令,称为阅读器碰撞;2)一个阅读器同时收到多个标签返回的数据,称为标签碰撞。在实际应用中,最容易出现标签碰撞,解决标签碰撞问题的算法称为标签防碰撞算法^[2]。在 RFID 系统中,应用最广泛的两类防碰撞算法分别是基于 ALOHA 的随机性防碰撞算法和基于二进制的确定性防碰撞算法。这两种算法都是基于时分多址(TDMA)的防碰撞算法。二进制树搜索算法的标签识别率可以达到 100%,但是复杂度高,收敛速度慢,识别时间长;ALOHA 算法的复杂度较低,识别速度快,受系统中标签数目影响较小,但是识别效率不高^[3]。

EPC global 提出的 EPC-C1G2 中采取了 Q 值防碰撞算法^[4]。该算法通过统计识别帧内部空闲和碰撞时隙的数目,来调控下一个识别帧的长度,使系统在不同的标签数目下,均能保持较好的识别性能。目前,对于 Q 值算法的研究主要集中在以下几个方面:

1)对帧长调整的阈值进行改进。任守纲等^[5]通过增加计数器分别计算碰撞和空闲的时隙个数,单独处理碰撞时隙和空闲时隙,并将两个计数器的差值与门限阈值进行比较,以动态调整 Q 值。他们还将单一参数 C 分解为两个权重参数,分析了在不同条件下两个权重参数的最优值^[6]。王进等^[7]提出了根据变化的标签数目自适应修改 Q 值,分化 C 值以调整帧长度。Zhu 等^[8]针对 Q 变化时的帧长不适应问题,提出了一种新颖的 Q 值防碰撞算法。

2)提升标签估算能力。付钰等^[9]利用马尔可夫时隙模型,分析了不同连续时隙状态下帧长与标签数目的关系,提出了一种基于连续时隙预测的防碰撞算法。张学军等^[10]通过监测一定数目的标签响应时隙状态来分析连续碰撞时隙和空闲时隙,以快速调整帧的大小。

到稿日期:2017-07-01 返修日期:2017-10-12 本文受国家自然科学基金项目(61761004),广西自然科学基金面上项目(2015GXNSFAA139290),广西科学研究与技术开发计划项目(桂科攻 14124005-2-3)资助。

杨子薇(1993—),女,硕士生,主要研究方向为多媒体通信网络理论与技术;郑嘉利(1979—),男,教授,主要研究方向为多媒体通信、物联网技术, E-mail: zhengjiali@vip.163.com(通信作者);岳世彬(1992—),男,硕士生,主要研究方向为多媒体及其网络工程;袁源(1995—),女,硕士生,主要研究方向为多媒体通信网络理论与技术;石静(1992—),女,硕士生,主要研究方向为多媒体通信网络理论与技术。

3)对标签进行分组。潘思丞等^[11]提出了静态分组的算法;李建雄等^[12]提出了将标签分组与动态调整 Q 值相结合的算法。

针对上述算法比较单一以及在大量标签的情况下不能较好地维持稳定的系统效率的问题,本文提出了一种基于 SCHOUTE^[13]标签分组的改进型 Q 值防碰撞算法。此算法首先预测标签数据,若标签数目较多则进行分组操作,然后对分组后的数据分别使用改进的 Q 值算法,通过计算当前帧长的动态门限,将原 Q 值算法中判断 Q 值是否改变改为判断 2^Q 改变的范围,从而对帧长进行调整。仿真结果表明,此算法不仅解决了大量标签的识别效率问题,同时解决了 Q 变化时的帧长不适应问题,提高了系统的实际吞吐率,减少了识别时间和时隙数。

2 Q 值防碰撞算法

2.1 Q 值算法的具体流程

为了进一步提高系统的识别效率,加快识别速度,EPC-C1G2 标准规定了一种基于 Q 值的防碰撞算法,该算法属于 ALOHA 算法的一种。这种算法的特点是帧长为 2^Q ,通过判断识别帧内空闲和碰撞时隙的数目,结合步长 C 来调整 Q 值,从而能够使帧长达到最佳值,使系统在不同的标签数目范围内均能保持比较好的识别性能。

Q 值防碰撞算法的具体步骤如下。

1)阅读器首先发送 Query 命令,该命令中含有一个参数 Q,接收到命令的标签可在 $[0, 2^Q - 1]$ 范围(称为帧长)内随机选择时隙,并将选择的值存入标签的时隙计数器中,只有计数器为 0 的标签才能响应,其余标签保持沉默状态。

2)当有且仅有一个标签响应时,标签与阅读器建立通信,退出这轮盘存,其他标签接收阅读器发送 Query Rep 命令,并将各自的时隙计数器减 1,若减为 0,则给阅读器发送一个应答信号。

3)当没有标签响应或者有多个标签响应时,读写器相应地使用步长 C 来对 Q 值进行调整,在调整之后,判断新的 Q 值相比原 Q 值是否发生了变化,若发生变化,则结束当前帧,通过 Query Adjust 命令调整 Q 值,让所有标签重新产生随机数。

EPC Class1 Gen2 标准中提供了一种参考算法来确定 Q 值的范围。其中, Q_{fp} 为浮点数,其初值一般设为 4.0,对 Q_{fp} 四舍五入取整后得到的值即为 Q; C 为调整步长,其典型的取值范围是 $0.1 < C < 0.5$,通常当 Q 值较大时, C 取较小的值,当 Q 值较小时, C 取较大的值。

因此,当第 i 帧结束时,对 Q_{fp} 取整并调整 Q_{i+1} ,得:

$$Q_{i+1} = \text{round}(Q_i + C(N_c - N_e)) \quad (1)$$

其中, N_c 和 N_e 分别表示第 i 帧中碰撞和空闲时隙的数目, $\text{round}(x)$ 表示接近 x 的最小整数。

2.2 标签识别率的分析

在 RFID 系统中,标签识别率的高低决定了系统的性能。标签识别率被定义为只有一个标签选择的时隙数目与系统全部时隙数目的比值。而系统的总时隙数目包括:只有一个标签选择的成功时隙、没有标签选择的空闲时隙和多个标签选择的碰撞时隙。因此,标签识别率 S 为:

$$S = \frac{N_s}{N_s + N_c + N_e} \quad (2)$$

其中, N_s 表示成功时隙, N_c 表示碰撞时隙, N_e 表示空闲时隙。

ALOHA 防碰撞算法的系统效率取决于时隙数与标签数的关系,当标签数较小时,空闲时隙较多,系统效率较低;当标签数大于时隙数时,碰撞时隙多,系统效率也较低。可以证明,当标签数约为时隙数时,系统的吞吐率达到最大值。

假设待识别的标签数为 n,帧长为 L,标签随机选择 $[0, L]$ 范围内的随机数,第 i 个时隙中的标签数为 m,所有标签选择随机数的过程是相互独立的,那么标签选择时隙服从二项分布。则第 i 个时隙中有 r 个标签的概率 P 为:

$$P(m=r) = C_n^r \cdot \left(\frac{1}{L}\right)^r \cdot \left(1 - \frac{1}{L}\right)^{n-r} \quad (3)$$

当 $r=1$ 时,即第 i 个时隙中仅有一个标签,表示该时隙是成功时隙,此时概率 P 为:

$$P(m=r=1) = C_n^1 \cdot \left(\frac{1}{L}\right) \cdot \left(1 - \frac{1}{L}\right)^{n-1} \quad (4)$$

则一帧内有成功时隙的期望 E 为:

$$E(m=1) = L \cdot C_n^1 \cdot \left(\frac{1}{L}\right) \cdot \left(1 - \frac{1}{L}\right)^{n-1} \quad (5)$$

系统的吞吐率 η 为:

$$\begin{aligned} \eta &= \frac{E(m=1)}{L} = C_n^1 \cdot \left(\frac{1}{L}\right) \cdot \left(1 - \frac{1}{L}\right)^{n-1} \\ &= \frac{n}{L} \cdot \left(1 - \frac{1}{L}\right)^{n-1} \end{aligned} \quad (6)$$

对 n 求导以求其极点,得:

$$L = \frac{1}{1 - e^{-\frac{1}{n}}} \approx \frac{1 + \frac{1}{n}}{1 + \left(\frac{1}{n} - 1\right)} = n + 1 \quad (7)$$

分析表明,当标签数目 n 约为帧长度时,系统的识别率达到最大。

$$S_{\max} = \frac{n}{L} \left(1 - \frac{1}{L}\right)^{n-1} \approx \frac{n}{L} e^{-\frac{n}{L}} \approx 0.367 \quad (8)$$

但由于 RFID 系统的硬件条件,当环境中大量的标签时,帧长不能够无限地增加,因此本文先对标签采取分组操作,通过减少响应的标签数量来降低标签之间的碰撞率,从而提高系统的识别率。定义分组数 G 为:

$$G = \frac{\text{未识别标签数}}{\text{帧长}} \quad (9)$$

不同帧长所对应的系统效率如图 1 所示。

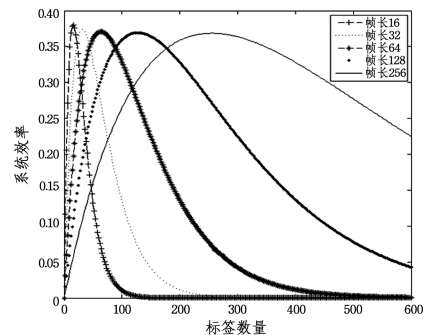


图 1 不同帧长的系统效率

Fig. 1 System efficiency of different frame lengths

根据抛物线的对称性可知,相邻的两个帧长中必然存在

识别效率相同的点,即 $\eta_L = \eta_{2L}$ 。将其代入式(6),求得交点的标签数为:

$$n = \frac{\ln 2}{\ln((2L-1)/(2L-2))} + 1 \quad (10)$$

由于实际应用中标签数量较大,因此令帧长 L 为目前实际允许的最大帧长 256,将 $L=256$ 代入式(10),得出需要分组的临界标签数为 354。因此,当 $L=256$ 时,为了保证系统有较好的识别率,阅读器最多可以识别 354 个标签,故当标签数小于 355 时,直接采用改进的 Q 值算法;当标签数大于 355 时,对标签进行分组。

在实际应用中,结合基本帧时隙算法,可以得出如表 1 所列的标签数 n 与分组数 G 的对应关系。

表 1 不同标签数的分组情况

Table 1 Groupings of different labels

标签数 n	分组数 G	分组情况
0~354	1	
355~610	2	256,99~354
611~866	3	256,256,99~354
866~1122	4	256,256,256,99~354
...

SCHOUTE 基于泊松分布提出了一种针对动态帧时隙算法的标签评估体系。未识别的标签数 n_0 可以通过下式得到:

$$n_0 = 2.39N_c \quad (11)$$

该方法的原理简单,移植方便,对硬件的要求较小,能够较为准确地估计标签数目。

3 Q 值改进算法

传统 Q 值算法的效率会在识别过程中的某处突然下降,其原因是:当标签数目较多时, Q 值的变化过大,导致与最佳帧长相差较大,从而降低了系统效率。因此,本文对 Q 值算法进行改进,将原 Q 值算法中对 Q 取整后进行判断改为对 2^Q 进行判断,即当 2^Q 变化到一定程度时再对帧长进行调整。

门限 μ 由式(12)确定:

$$\mu = \begin{cases} 2^Q * a, & Q_{fp} < Q \\ 2^Q * b, & Q_{fp} > Q \end{cases} \quad (12)$$

其中, a 表示当 $Q_{fp} < Q$ 时,门限值所选取的参数; b 表示当 $Q_{fp} > Q$ 时,门限值的参数。这两个参数与未读标签数相关,通过仿真实验获得。在 Python 中对相同未读标签数下的取值组合进行仿真,并在 Matlab 中绘图,其中步长 C 取值为 0.2。

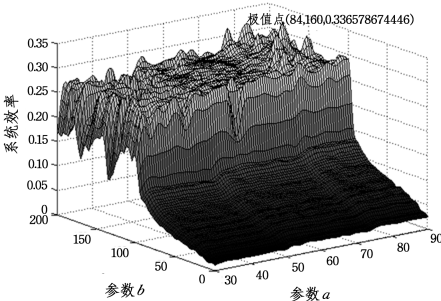


图 2 标签数为 100 的组合图

Fig. 2 Graph of label 100's combination

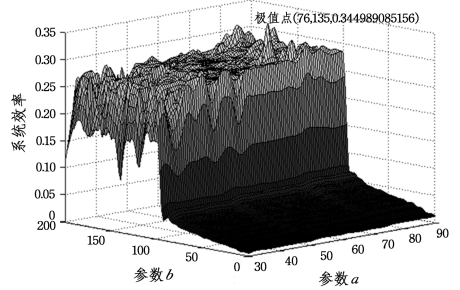


图 3 标签数为 200 的组合图

Fig. 3 Combination graph of 200 labels

图 2 和图 3 分别以标签数为 100 和 200 为例,给出了两个参数 a 和 b 的组合。从图 2 中可以看出,当取值组合为 (0.84, 1.60) 时,系统效率达到最大值,为 33.66%。从图 3 中可以看出,当取值组合为 (0.76, 1.35) 时,系统效率达到最大值,为 34.50%。由此,结合标签分组依据,可以得出不同的未读标签数段内的最佳系数值,如表 2 所列。此处求取的参数是所列标签范围内的平均值。

表 2 不同标签数范围的系数组合

Table 2 Coefficient combination of different number of labels

标签数范围	参数 a (平均值)	参数 b (平均值)	系统效率
0~40	0.58	1.80	0.34
40~80	0.84	1.55	0.34
80~120	0.78	1.40	0.30
120~160	0.84	1.40	0.34
160~200	0.76	1.35	0.34
200~240	0.84	1.45	0.33
240~280	0.82	1.40	0.35
280~320	0.78	1.70	0.33
320~360	0.82	1.40	0.35
360~400	0.90	1.60	0.36

通过分析表 2 中的数据可以得出,当标签数较少时,两个参考系数的值存在较大波动,随着标签数量的增加,两个参考系数的值逐渐趋于稳定,其中,参数 a 在 0.80 左右波动,参数 b 在 1.50 左右波动。对此,我们可以近似认为,当标签数大于 200 时,可以直接使用系数 $a=0.80, b=1.50$ 来计算相应的门限值,由此可以快速改变相应的帧长,使得帧长能够快速达到收敛值,提高系统的效率。

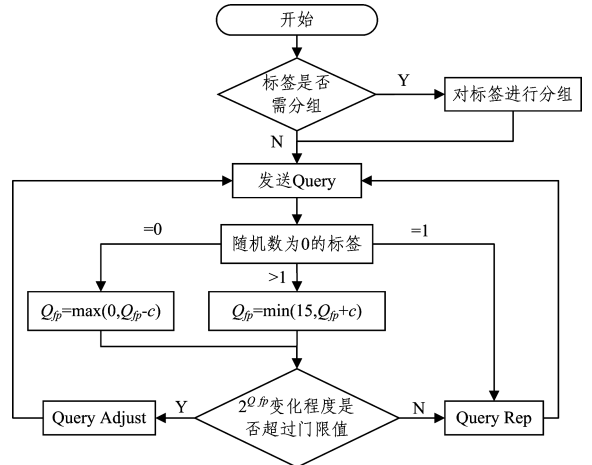


图 4 改进的 Q 值算法的流程图

Fig. 4 Flowchart of improved Q value algorithm

通过实验仿真能够看出,在大量标签的情况下,读写器的读取时间增加,系统的效率有所降低并且波动幅度较大。为此,结合前文所提到的分组方式,先对标签进行一轮识别,估算标签的数目,若标签数量大则进行分组,再对分组后的标签进行识别,具体流程如图 4 所示。

4 实验结果分析

本文使用 Python 2.7 来模拟仿真算法,使用 Matlab2014a 对得到的实验数据进行分析作图。衡量算法性能指标主要是识别相同标签数所消耗的总时隙、总时间以及系统的吞吐量。

图 5 和图 6 分别从时隙消耗和系统吞吐量两个方面,给出了本文算法与传统 Q 值算法以及固定帧长为 128 和 256 的帧时隙算法的比较结果。图 7 从系统消耗时间方面,给出了本文算法和传统 Q 值算法的比较结果。

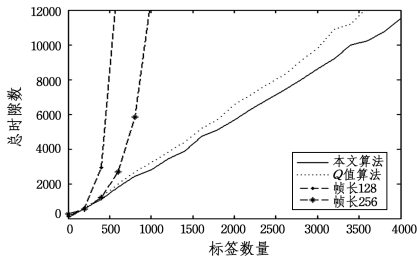


图 5 时隙消耗的对比如

Fig. 5 Contrast of slot consumption

从图 5 可以看出,相比于传统 Q 值算法和固定帧长为 128 和 256 的帧时隙算法,本文提出的标签分组算法在识别相同标签数的条件下,所消耗的总时隙数较少。并且相比于传统 Q 值算法,本文算法所消耗的总时隙数较为稳定并且减少了 15.1%。

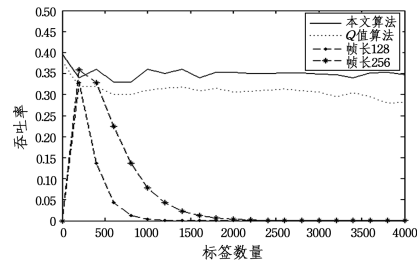


图 6 系统效率的对比如

Fig. 6 Contrast of system efficiency

从图 6 可以看出,相比于其他算法,本文算法在系统效率方面较其他算法有所提高;相比于传统 Q 值算法,本文算法在系统效率方面提高了 13.6%,并且拥有较为稳定的系统效率。

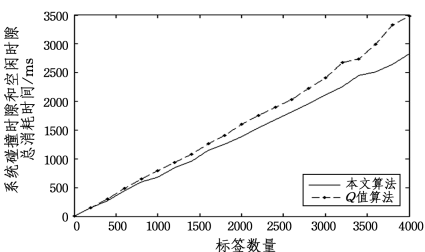


图 7 系统碰撞时隙和空闲时隙的总消耗时间

Fig. 7 Total consumption time of system collision slots and idle time slots

从图 7 中可以得出,识别同样的标签数量,本文算法较传统 Q 值算法在碰撞和空闲时隙所消耗的时间上有较好的改进效果,时间约缩短了 12.2%。

本实验中,标签个数均为 4000,所有结果都是经过 1000 次仿真所求得平均值。

结束语 本文在标签分组的基础上,提出了一种新颖的 Q 值防碰撞算法,首先对标签进行估算分组,然后对分组后的标签使用改进的 Q 值算法,当 2^Q 变化的程度超过门限值时,改变 Q 值的大小,从而调整帧长使其快速达到最佳值,通过仿真实验得出,本文算法在系统效率和稳定性方面都有所提升,相较于传统 Q 值算法,所消耗的时隙数减少了 15.1%,系统效率提高了 13.6%,空闲和碰撞时隙所消耗的时间缩短了 12.2%。特别是对于大量标签,本文算法在进行分组后可以节省读写器的消耗,能够对标签进行快速识别,在实际生活中有更广泛的应用前景。后续工作可以在如何优化门限值、提高读写器的效率等方面进行研究。

参考文献

- [1] ZHENG J L, QIN T F, et al. Tree-based backoff protocol for fast RFID tag identification[J]. Journal of China Universities of Posts & Telecommunications, 2013, 20(2): 37-41.
- [2] SHAN P F, ZHENG J L, YUE S B, et al. Enhanced Four - fork Tree RFID Anticollision Algorithm[J]. Computer Science, 2016, 43(S2): 271-274. (in Chinese)
单朴芳, 郑嘉利, 岳世彬, 等. 增强型四叉树 RFID 防碰撞算法 [J]. 计算机科学, 2016, 43(S2): 271-274.
- [3] DENG D J, TSAO H W. Optimal Dynamic Framed Slotted ALOHA Based Anti-collision Algorithm for RFID Systems[M]. Massachusetts: Kluwer Academic Publishers, 2011.
- [4] EPC global Inc. EPC Radio-frequency Identification Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860~960 MHz, Version 2.0.1. [EB/OL]. (2015-04-23). [2017-06-15]. <https://www.sogou.com/link?url=hedJjaC291NB9sv9GWONl-rVzfrU97rkh2HUvSwDqVvZRMSSyiv01cs02Xn2rX5SelfVVPvvSTzVDSrKSK2DBwrWfAAEGLHNwVKkTmhFA>.
- [5] REN S G, YANG F, WANG H Y, et al. Decision Threshold-based Q Algorithm for RFID Anticollision[J]. Computer Science, 2014, 41(8): 154-157. (in Chinese)
任守纲, 杨帆, 王浩云, 等. 基于判决门限的 RFID 防碰撞 Q 值算法[J]. 计算机科学, 2014, 41(8): 154-157.
- [6] REN S G, YANG F, XU H L. Research on Double Weight Parameter Anti-collision Q Value Algorithm in RFID System[J]. Computer Science, 2014, 41(4): 256-259. (in Chinese)
任守纲, 杨帆, 徐焕良. 一种双权重参数的 RFID 防碰撞 Q 值算法研究[J]. 计算机科学, 2014, 41(4): 256-259.
- [7] WANG J, YI L Z, WANG G P, et al. Research on an Enhanced Anti-Collision Algorithm for RFID[J]. Computer Engineering and Science, 2011, 33(6): 182-185. (in Chinese)
王进, 易灵芝, 王根平, 等. 新型 Q 值防碰撞算法在 RFID 系统中的研究[J]. 计算机工程与科学, 2011, 33(6): 182-185.

表2 导致摄像头崩溃的字段记录

Table 2 Field records resulting in crash of camera

设备	字段	描述	个数
Hikvision (DS-2CD7153-E)	CSeq Range	CSeq 中含特殊字符';', Range 字段值字符超长	2 (Range 为已公布)
Tiandy (TC-NC9200S3E- 2MP-E-IR30)	URL	Describe 方法中 url = rtsp://192.168.12.2dos: dos5545454 * 18//a * 1024 RTSP/1.0	1
Linksys (WVC54GCA)	Content	Setup 方法中 Content = 'A' * 120009	1

结束语 本文以 Hikvision, Tiandy 和 Linksys 的某些型号设备为研究对象进行测试,对捕获的样本集去重,并针对 boofuzz 框架的测试用例生成方法进行改进,通过构造 RTSP 协议状态图,使用基于深度优先遍历的方式遍历协议状态图,使在生成测试用例时遍历的路径更有效,生成的有效测试用例占比更高,执行时间更少。在执行测试用例过程中使用 TCP 3 次握手连接的原理来判断测试目标是否崩溃,以使监控模块在对 RTSP 进行模糊测试的过程中记录异常包时的精确性更高,减少了假死情况的记录。另外,在监控过程中实现远程监控,使记录的异常测试用例中没有过多的冗余,以便后续重放时减少因冗余产生的耗时。本文利用提出的模糊测试方法对上述 3 个品牌的监控设备进行测试,其不仅发现了已有漏洞,而且还发现了 3 个之前未被发现的导致摄像头直接崩溃的异常字段,并在得到结果后重放,进行了进一步确认。本文的不足之处在于针对复杂协议,该方法覆盖执行路径的效率较低,下一步需针对构造的协议状态图进行优化,使其适应面更广,效率更高。

参考文献

- [1] SHI F Y, FU D S. A survey on analysis and utilization of buffer overflow vulnerability[J]. Journal of Computer Science, 2013, 40(11): 143-146. (in Chinese)
史飞悦, 傅德胜. 缓冲区溢出漏洞挖掘分析及利用的研究[J]. 计算机科学, 2013, 40(11): 143-146.
- [2] MEI H, WANG Q X, ZHANG L, et al. Analysis of the progress of software technology[J]. Chinese Journal of Computers, 2009, 32(9): 1697-1710.
- [3] CHI Q, LUO H, QIAO X D. A survey of vulnerability mining and analysis technology[J]. Computer and Information Technology, 2009(Z2): 90-92. (in Chinese)
- [4] MA R, JI W, HU C, et al. Fuzz testing data generation for network protocol using classification tree[C]// Communications Security Conference. IET, 2014: 1-5.
- [5] MA R, WANG D, HU C, et al. Test data generation for Stateful network protocol fuzzing using a rule-based state machine[J]. Tsinghua Science and Technology, 2016, 21(3): 352-360.
- [6] KIM S J, JO W Y, SHON T. A novel vulnerability analysis approach to generate fuzzing test case in industrial control systems [C] // IEEE Information Technology, Networking, Electronic and Automation Control Conference. IEEE, 2016: 566-570.
- [7] HAN X, WEN Q, ZHANG Z. A mutation-based fuzz testing approach for network protocol vulnerability detection[C]// International Conference on Computer Science and Network Technology. IEEE, 2013: 1018-1022.
- [8] LI H, WANG S, ZHANG B, et al. Network protocol security testing based on fuzz[C]// International Conference on Computer Science and Network Technology. IEEE, 2015: 955-958.
- [9] WANG W, SUN H, ZENG Q. SeededFuzz: Selecting and Generating Seeds for Directed Fuzzing[C]// International Symposium on Theoretical Aspects of Software Engineering. IEEE, 2016: 49-56.
- [10] MA R, REN S, MA K, et al. Semi-valid fuzz testing case generation for stateful network protocol [J]. Tsinghua Science & Technology, 2017, 22(5): 458-468.
- [11] 胡昌振, 马锐, 纪文东, et al. Case generation method for semi-legalized fuzz test of network protocol based on finite-state machine: CN 105095075 A[P]. 2015.
- [12] NARAYAN J, SHUKLA S K, CLANCY T C. A Survey of Automatic Protocol Reverse Engineering Tools[J]. Acm Computing Surveys, 2015, 48(3): 1-26.
- [13] MA R, ZHU T, HU C, et al. SulleyEX: A Fuzzer for Stateful Network Protocol[M]// Network and Systems Security. 2017: 359-372.
- [14] 龚波, 冯军. 模糊测试——强制性安全漏洞发掘[M]. 北京: 机械工业出版社, 2009.
- [15] Sulley [EB/OL]. (2013-06-11) [2016-10-18]. <http://github.com/OpenRCE/sulley>.
- [16] RFC2326. RTSP Protocol [Z/OL]. (2009-08-10). <https://tools.ietf.org/html/rfc2326>.
- [8] ZHU B, WANG J, ZENG G. A non-integral-Q Algorithm for RFID system in anti-collision[C]// International Conference on Control, Automation and Robotics. IEEE, 2016: 374-377.
- [9] FU Y, QIAN Z G, MENG J, et al. FSA Anti-collision Algorithm Based on Continuous Slot Prediction[J]. ACTA Electronica Sinica, 2016, 44(9): 2081-2086. (in Chinese)
付钰, 钱志鸿, 孟婕, 等. 基于连续时隙预测的帧时隙 Aloha 防碰撞算法[J]. 电子学报, 2016, 44(9): 2081-2086.
- [10] ZHANG X J, MA J F, CHEN Y J, et al. An Enhanced Q Parameter Hybrid Anticollision Algorithm[J]. Computer Technology and Development, 2013(8): 47-51. (in Chinese)
张学军, 马军飞, 陈彦君. 增强型 Q 参数混合防碰撞算法[J]. 计算机技术与发展, 2013(8): 47-51.
- [11] PAN S C, WANG H Q, ZHANG X H, et al. Research in anti-collision algorithm of block ALOHA in static environment[J]. Computer Engineering and Applications, 2016, 52(20): 114-117. (in Chinese)
潘思丞, 王慧琴, 张小红, 等. 静态环境中分组 ALOHA 防碰撞算法研究[J]. 计算机工程与应用, 2016, 52(20): 114-117.
- [12] LI J X, FENG X, SHI W G, et al. RFID anti-collision algorithm based on dynamic Q method[J]. Journal of Tianjin Polytechnic University, 2015, 34(6): 55-60. (in Chinese)
李建雄, 冯鑫, 史伟光, 等. 基于动态 Q 值的 RFID 防碰撞算法[J]. 天津工业大学学报, 2015, 34(6): 55-60.
- [13] SCHOUTE F C. Dynamic Frame Length ALOHA[J]. Mobile Communications, 1983, 31(4): 565-568.

(上接第 155 页)