RFID 系统克隆标签检测方法综述

孔春明[1],黄茗涵[1],徐　鹤[2]
(1. 南京邮电大学 贝尔英才学院,江苏 南京 210023;
2. 南京邮电大学 计算机学院、软件学院、网络空间安全学院,江苏 南京 210023)

摘　要:随着物联网的发展和无线射频识别技术(radio frequency identification,RFID)的广泛应用,RFID 系统的安全问题越发突出。其中克隆标签的出现极大地阻碍了 RFID 系统的大规模发展,成为当前一个亟待解决的难题。通过总结分析目前 RFID 克隆标签检测领域的一些主流方法,旨在为后续研究更有效的 RFID 克隆标签检测策略奠定基础。针对目前已知的一些检测方法,该文将克隆标签检测方法归纳总结为射频指纹、同步秘密、轨迹分析和碰撞检测四大类,并较为系统地对这四大类方法所包含的具体策略进行了研究,同时对这些方法策略进行了横向与纵向的对比分析。目前这四类方法都存在一定的缺陷,导致其无法直接应用于现有 RFID 系统进行克隆标签检测或者应用条件较苛刻。针对目前这些方法存在的问题,认为匿名 RFID 系统克隆标签的分布式检测是未来的一个主要研究方向。

关键词:无线射频识别;克隆标签;射频指纹;同步秘密;轨迹分析;碰撞检测
中图分类号:TP309　　**文献标识码**:A　　**文章编号**:1673-629X(2022)08-0122-07
doi:10.3969/j.issn.1673-629X.2022.08.020

Overview of RFID System Clone Tag Detection Methods

KONG Chun-ming[1],HUANG Ming-han[1],XU He[2]
(1. Bell Honors School,Nanjing University of Posts and Telecommunications,Nanjing 210023,China;
2. School of Computer Science,Nanjing University of Posts and Telecommunications,Nanjing 210023,China)

Abstract:With the development of the Internet of Things and the wide application of radio frequency identification,the security problem of RFID system is becoming more and more prominent. Among them,the emergence of clone tags greatly threatens the life and property safety of producers and consumers,which has become an urgent problem to be solved. At present,some mainstream methods in the field of RFID clone tag detection are summarized and analyzed,aiming to lay the foundation for further research on more effective RFID clone tag detection strategies. According to some known detection methods,clone tag detection methods are summarized into four categories: radio frequency fingerprint,synchronization secret,trajectory analysis and collision detection. The specific strategies contained in these four categories are systematically studied. At the same time,these methods are compared horizontally and vertically,and the evaluation conclusions are shown in the form of tables. At present,these four methods have been found to have certain defects after analysis,which makes them unable to be directly applied to the existing RFID systematic clone tag detection or the application conditions are harsh. In view of the existing problems of these methods,the distributed detection of clone tags in anonymous RFID systems is identified as a direction that needs to be worked in the future.

Key words:radio frequency identification;clone tags;RF fingerprint;synchronization secret;trajectory analysis;collision detection

0　引　言

随着物联网的发展,无线射频识别技术(radio frequency identification,RFID)在生活中的应用也越发广泛,其被认为是 21 世纪最具发展潜力的信息技术之一。与原有的条形码、IC 识别等自动识别技术相比,RFID 技术由于其识别距离长、信息储量大、可同时识别多个目标、抗干扰能力强等优点得以快速发展与广泛应用。

一般的 RFID 系统有三个基本的组成部分,即 RFID 电子标签(Labels)、RFID 读写器(Reader)以及后端数据库服务器(Database),如图 1 所示。

图 1　RFID 系统构成

收稿日期:2021-09-12　　**修回日期**:2022-01-12
基金项目:国家自然科学基金(61602261)
作者简介:孔春明(2001-),男,研究方向为物联网技术;徐　鹤,副教授,CCF 会员(19957M),研究方向为物联网技术及应用。

尽管 RFID 技术的发展潜力巨大,但是 RFID 带来的安全问题也不容忽视,其中针对 RFID 系统的标签克隆攻击是当前研究的一个热点。克隆攻击是指将 RFID 电子标签或智能卡的信息复制到克隆标签中,使克隆标签具有与原标签相同的特性,可以进行替换。克隆攻击使用嗅探、窃听、物理篡改等手段获取原始标签的所有数据,包括编码和用户数据,将所有信息写入一个可以写入整个区域的 RFID 标签,并复制标签[1]。这里需要特别提一下,克隆标签不等同于伪造标签,Bu 等人的文章中[2]也特别指出了这一混淆,克隆标签的定义比伪造标签更严格,也可以理解为伪造标签可能存在某些与真正的标签不一致的秘密,但是克隆标签是与真正标签完全一致的。目前,处理标签克隆主要有两种方法:预防和检测。预防方法通过对标签采用加密技术、物理抗克隆函数、安全认证协议等方式[3-5]来防止标签克隆。然而,还没有一种方法宣称能完全抵御克隆攻击。此外,由于存储和计算能力的限制,一些预防方法无法在供应链使用的低成本标签中实现。因此,检测方法是处理低成本标签克隆问题的合适方法[6]。

该文主要的研究内容为标签克隆攻击的检测方法,即在克隆攻击已经发生的情况下,通过一定的手段识别出克隆标签并做出相应的响应。目前主流的检测克隆攻击的方法大致可以分为四大类:射频指纹(radio frequency fingerprints)、同步秘密(synchronized secret)、轨迹分析(trajectory analysis)和碰撞检测(collision detection),该文对这些基本的方法与具体的技术进行了研究,并做了横向与纵向的对比。

1　相关方法

1.1　射频指纹

射频指纹是指由于射频设备电子元器件的个体差异,导致其发射出的电磁波包含设备的独特特征,人们形象化地将这种与具体设备相关联的物理层上的模拟和数字信号特征称为“射频指纹”。由于设备制造过程的差异性,没有两个设备是完全相同的,它们发射出的射频信号的特征也不完全相同,因此可以通过“射频指纹”对设备进行识别和认证。由于射频指纹的特征与设备的物理层硬件特征紧密相关且不可人为控制,从而可以据此检测克隆行为的发生。

文献[7]中指出像电子产品代码(EPC)、标识符(ID)等应用层信息容易被攻击者克隆,但是对射频信号的物理层信息却很难去克隆,这是因为射频信号很容易受到环境因素和硬件条件的影响,其值难以预料。作者针对静态场景和动态场景分别使用基于聚类和基于邻居的方法进行克隆检测,检测效果较好。此方法不需要任何软件重新设计和硬件扩充,只需要基于现有的 COTS RFID 设备即可,但是此方法似乎只能检测到克隆攻击发生并统计出克隆标签的数量,无法具体区分出哪些标签是克隆标签。

同时发明专利中[8]使用的是 RFID 相位指纹进行 RFID 标签克隆检测,方法就是使用 RFID 相位提取工具对所有 RFID 标签进行相位采集处理,通过最小二乘法进行减噪操作,继而建立优化指纹库,然后检测时只需要将测量到的标签指纹与指纹库中的指纹进行比对即可准确识别克隆标签。专利中没有提到该方法的实际效果,但笔者认为这种方法的准确率可能不高,而且对于相位提取工具和后续减噪优化操作的要求会比较高。而 Zhang 等人的论文中[9]则具体地介绍了一种基于物理层特性地射频指纹识别方法“牵星法”,使高频 RFID 卡与其唯一且不可克隆地射频特征紧密绑定。该方法在初始化阶段首先将所有的 RFID 卡分为星卡和发行卡两类并建立关系对,然后通过线性判别式分析(LDA)算法对 n 个关系对进行训练。在检测阶段,只需要将待检测标签与 n 个参考对象进行多次两两识别,大幅降低了识别难度。同时该识别系统仅由一个天线、一个读卡器和一个示波器组成,结构简单。

1.2　同步秘密

Mikko Lehtonen 等人的文章中[10]首次讨论和评估了将同步秘密(synchronized secrets)应用到标签克隆检测领域。所谓同步秘密,其实就是一个伪随机数,也可以理解成一个一次性密码。这种方法理解起来很简单,在标签的可重写内存中写入一个随机数,每次读取标签时都会更改该数,同时要注意后端不会擦除旧的秘密,这样做是为了检查标记是否因为被克隆或仅仅因为同步错误而无法通过。一个集中的后端系统发布这些随机数并跟踪哪个随机数写在哪个标签上以检测同步错误。每次读取标签时,后端首先验证标签的静态标识符(UID)。如果此数字有效,后端会将标签的同步秘密与为该特定标签存储的秘密进行比较。如果这些数字匹配,则 标签通过检查——否则会触发警报。检查后,后端生成一个新的同步秘密,读取器设备将其写入标签。

这种检测方法存在一个比较严重的问题:过时的同步秘密并不完全意味着克隆已经发生。前面提到在更新随机数时,原来旧的随机数并不会擦除,而是会留在后端中。所以如果标签具有过时的同步秘密,则标签是真实的但尚未正确更新(去同步),或者有人故意获取旧秘密并将其写入正版标签(复杂的故意破坏,Mikko Lehtonen 称这种破坏形式在当今的商业 RFID 应用中显得有些不切实际),或者正版标签已被克隆

并且克隆的标签已被扫描。针对去同步错误,Obinna Stanley Okpara 所写的文章中[11]尝试引入 ACK 消息来进行解决:在验证之后,标签向读卡器发送一个 ACK,表明它已经同步并拥有新的秘密。作为响应,读取器向后端发送一个 ACK,表明它从标记中获得了 ACK 消息。最后,后端向读取器发送其 ACK 消息,以确认整个确认过程已成功完成。这有点类似于传输控制协议(TCP)三次握手。不过虽然引入了 ACK 消息,但是仍不能确保在最短时间内收到 ACK,读卡器和后端之间的距离、电磁干扰(EMI)的存在等因素会影响 ACK 传输时间,这将导致需要在短时间内对大量标签进行身份验证的 RFID 系统会有明显的延迟。同时,同步秘密这一方法还存在一些其他的缺陷,比如它要求标签拥有可重写的内存空间,而且这种检测方法只能定位具有相同标识符的对象,但仍需要与人工检查一起使用以确定哪些对象不是真品。Obinna Stanley Okpara 在文章的最后也写道“本质上,同步秘密在 RFID 应用中不是一种有效的方法。”

使用 ACK 消息标记同步秘密更新如图 2 所示。

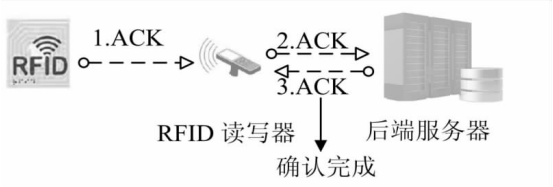

图 2 使用 ACK 消息标记同步秘密更新

1.3 轨迹分析

根据标签轨迹的时空相关性分析,Huang 等人提出了一种基于 Floyd-Warshall 算法和时空碰撞的自适应克隆检测方法(ACD)[1]。所谓时空碰撞,简单来说就是短时间内同一个标签出现在两个相距很远的地方。该方法首先通过统计方法获得相邻节点之间的时空关系,然后基于最短路径算法 Floyd-Warshall 计算得到任意节点之间的时空关系。接着对所有节点进行综合,得到相邻节点之间的最短时间矩阵。将实时数据与最短时间矩阵 dis 数据进行比较,可以实现对克隆标签的检测。在实时采集的日志中,当两条相邻的 ID 相同的记录之间的时间间隔小于 dis 的时间间隔时,系统认为存在异常,并触发警报。管理员将知道克隆标记的位置和 ID。这种方法可以直观、准确地实时显示异常标签的位置。它使用商用现货 RFID 设备,不需要额外的硬件资源。当然,这个方法也存在一些问题,比如忽略了数据冗余、没有考虑实际环境的复杂性等。

后面 Huang 等人的团队针对这些问题又对 ACD 方法进行了改进,提出了一种名为 DeClone 的基于轨迹的概率检测方法[12]。DeClone 增加了数据预处理环节,使用有限状态机去清理冗余的数据。然后数据跟踪将原始 RFID 数据流转换为轨迹数据。DeClone 方法采用的时空关系建模也与 ACD 方法不太一样,研究者对不同时间段的实时轨迹进行了建模,将一个长时间帧分割成多个小时间窗口,对每个时间窗口中相邻节点之间的可达时间进行 gamma 分布拟合,并通过置信区间的下界确定相邻节点之间的最短可达时间,这比 ACD 的可到达时间的最小值作为固定阈值更准确一些。检测阶段研究者将实时轨迹划分为多段。然后,将一段轨迹与相应的最短可达时间进行比较,以检测异常。另外,累计异常阈值的提出使得该方法在不同场景下的适用性提高,根据不同场景下精度和召回率的要求不同选择适当的阈值可以较好地达到预期要求。不过,DeClone 在某些方面仍有一些局限性。首先,该方法设想的应用场景是展览会等克隆标签与真实标签同时同地出现的应用场景,但是成功克隆标签后,克隆标签和真实标签可能不会在 RFID 系统中共存。其次,DeClone 检测到克隆标签后,无法准确区分真实标签和克隆标签。

以上两种方法所用到的轨迹都是基于某一场景的,Luo 等人提出了一种针对物流供应链的标签克隆检测方法[13-14]。文章针对现有分析模型存在的分析维度单一、数据量不足、无法区分异常等缺陷,从历史来源、规模数量、位置变化、库存时间等方面提出一种多维 RFID 供应链异常检测模型。同时对供应链上货物规模数量的一致性、逻辑的一致性进行检测(包括前后站点一致性、局部路径的一致性和停留时间的一致性),使 RFID 克隆标签检测具备区分异常类型的能力,相较于现有的检测模型,提高了异常检测的准确率。

Luo 所提出的基于供应链的检测方法需要从物流公司或者物流站点获取样本的数据,对于产品信息流的要求比较高,而 Li 等人提出的双轨迹克隆检测法则显得更加地简单[15],该方法不依赖于任何预先定义的供应链结构或正确的产品信息流,使得其面对供应链的动态变化具有灵活性,便于普遍部署。所谓“双轨迹”,第一条轨迹是由验证序列构成的,该方法通过在标签中写入验证序列,使得随着标签随产品在供应链中流动,正版标签和克隆标签因验证序列的不断更新而出现不同,而且标签中的验证序列随时间变化会呈现一定的规律,于是形成一条序列轨迹;第二条轨迹是结合标签事件信息中业务动作(如接收或者运输)的一致性形成的轨迹。该方案通过评估 2 条轨迹的正确性来发现克隆,在评估克隆存在时充分考虑了标签误读、误写、事件丢失以及错误运输。

1.4　碰撞检测

克隆标签是对合法标签的完全复制,它具有合法标签的全部信息,包括全球唯一号,所以当接收到阅读器发出的命令时,克隆标签和合法标签会得到相同的值,也就是说它们会在同一个时隙中进行回复,这种冲突不能通过选择不同的随机种子来解决。基于这一事实,可以为每个合法标签分配一个单一时隙,在阅读器端,如果这一单一时隙变成了冲突时隙,那么就可以确定在该时隙回复的合法标签受到了克隆攻击[16]。

Bu 的团队在碰撞检测方面做了许多的研究与尝试,起初,他们的想法是利用广播和冲突来识别克隆标签[17-18]。其基本的思路为当读卡器广播只指定一个标签来发送响应的查询消息时,如果读卡器接收到多个响应的冲突,就可以认为克隆的标记存在。考虑到广播 ID 很耗时间而且不利于隐私的保护,于是 Bu 的团队采用时隙 Aloha(SLOTTED-ALOHA)来指定标签以在不广播其 ID 的情况下进行响应。每个标签根据阅读器广播的参数信息以及自己的 ID 进行哈希运算选择其应答的时隙,阅读器根据标签的实际应答情况,组建一个实际时隙状态向量(0 或 1),通过时隙状态向量的值就可以判别是否存在克隆标签。该协议通过多轮的执行,直至 RFID 系统中所有标签被识别。

然而,上述克隆标签识别方法的前提是克隆标签百分百回复阅读器即攻击概率为 100%。当克隆标签以一定的概率发起攻击时,该方法就会出现大量的误判,导致识别精度快速地下降,识别效率低。针对这一缺陷,Chen 等人的发明专利中[19]为克隆标签引入了攻击概率的概念,提出了一种更具有实际性的概率性克隆攻击模型。阅读器采用多种子和帧时隙 Aloha 结合的方式提高了帧中单时隙的比例,只有当真实标签在期望帧中选中单时隙时,才能根据该单时隙在实际帧中的状态对真实标签是否被克隆做出判断。这种基于多种子技术对克隆标签进行识别,不仅可以识别概率性的克隆攻击,也适用于每个克隆标签都具有 100% 攻击概率的情形,更具有普适性。

后面 Bu 的团队又研究了匿名 RFID 系统的确定性克隆检测问题[20],提出了 BASE、DeClone 和 DeClone+等快速确定性克隆检测协议。BASE 利用克隆标签会使标签基数超过 ID 基数的这一性质来检测克隆标签的存在。DeClone 主要设计方法为将 slotted Aloha 协议和 tree traversal 协议结合起来检测由克隆标签导致的不可调和的信息冲突,它强制在每个插槽中进行克隆检测,以提高大型系统的克隆检测速度。DeClone+为 DeClone 的优化版本,其设计的动机是更多的克隆导致更容易检测。它所做出的改进是可以根据给定的 ID 基数 n 和克隆 ID 基数 m 通过公式计算出一个最小的帧大小来满足所需的检测精度,而不是像之前的方法中直接设置默认帧大小。对于克隆标签较多的场景具有更快的检测速度。

Bu 的团队的方法中采用的大多是时隙 Aloha 防碰撞协议,Guo 的文章中[21]指出采用 Aloha 防碰撞算法检测克隆标签很难保证真实标签和对应的克隆标签每次同时出现在一个时隙,所以采用基于 Aloha 防碰撞协议就有可能存在漏检问题。而如果采用基于树的防碰撞协议,若存在两个一样 ID 的标签,它们永远同时响应,即出现不可调解的碰撞。Guo 采用基于多叉树防碰撞算法的克隆检测方法,提出了一个快速 RFID 克隆攻击检测方法 MT-CAI。其使用自适应四叉剪枝查询树防碰撞协议(A4PQT)自适应地剪去四叉树的空闲时隙,使之分裂叉数趋近于 3。当产生碰撞时隙时,MT-CAI 会检测曼彻斯特编码的跳变情况。如果在某些位出现无状态跳变,则说明是可调解的碰撞,此时阅读器根据剪枝原则更新查询前缀,继续下一轮的查询;如果发生碰撞,曼彻斯特编码的跳变依旧是正常的,则说明出现不可调解的碰撞,这就表明存在克隆标签。

以上方法虽然都声称适用于大型 RFID 系统,但是似乎都没有提到在多个阅读器并存的情况下如何快速查找待检测阅读器覆盖范围内的所有标签。Feng 的文章[16]中提出了一种大规模系统中快速识别克隆标签算法 CAIP,他提出利用布鲁姆过滤器快速查找待检测阅读器覆盖范围内的所有标签,然后利用多个 Hash 函数为每个标签分配一个单一时隙,阅读器通过检测各时隙的状态来判断标签是否受到克隆攻击。

HazalilaKamaludin 等人提出了一种基于双哈希冲突的一致性和改进的 Count-Min Sketch 向量的克隆标签识别方法[22],使用散列将流数据中的项目映射到一个小空间草图向量上,该向量可以轻松更新和查询。该方法依赖于不同 Count-Min Sketch 向量中两个哈希函数的哈希冲突的一致性来揭示克隆的存在。作者认为,攻击者在真标签准备就绪后创建克隆标签,因此,克隆标签的标签读取频率合理地低于真标签。所以,如果发生散列冲突并且在两个 Count-Min Sketch 向量处存在相同的 EPC,则不断更新读取频率可以精确地确定克隆标签存在于哪个读取器,这是之前的方法中未提及的。

2　对比分析

为了对所读文献中采用的不同方法进行比较和评价,选用了五个指标进行具体地评估与分析,如表 1 所示。这五个指标分别为安全性、是否为轻量级、集中式/分布式、算法复杂度、能否区分真实标签和克隆标

签。其中,安全性又分为可抵御的攻击类型、准确性和隐私性三个方面,这里的隐私性主要是对 RFID 系统是可识别系统和匿名系统做出区分;是否为轻量级主要是从对软硬件设备、供应链结构、数据信息等环境因素的依赖程度角度进行评判;集中式和分布式的区别来自于克隆标签和它对应的真实标签是否应该在同一系统中被检测,集中式即服务器收集全局标签数据用于克隆检测,而分布式即阅读器可以基于标签中的某些共享秘密独立检测克隆标签,无需求助于所有标签的全局知识;能否区分真实标签和克隆标签即部分方法只能用于检测系统中是否存在克隆标签,无法区分真实标签和克隆标签,而另一部分方法却可以做到。

表 1 各方法对比

类型	文献方法	安全性			轻量级	集中式/分布式	算法复杂度	能否区分真实标签和克隆标签
		可抵御的攻击	准确性	隐私性				
射频指纹	Combating Tag Cloning with COTS RFID Devices[7]	未增强原系统抵御攻击的能力	静态场景下 99.8% 动态场景下 99.3%	可识别系统	是(无需任何硬件和软件修改且兼容 G1 G2 协议)	集中式	$O(n)$	能
	一种快速克隆 RFID 标签检测方法[8]	未增强原系统抵御攻击的能力	高	可识别系统	是	集中式	$O(n)$	能
	牵星法[9]	未增强原系统抵御攻击的能力	等错误率 EER=2.5%	可识别系统	是	集中式	$O(n)$	能
同步秘密	Securing RFID Systems by Detecting Tag Cloning[10]	中间人攻击 重放攻击 恶意代码注入	99.15% 的克隆标签会触发警报	可识别系统	是	集中式	$O(1)$	能
	Detecting Cloning Attack in Low-Cost Passive RFID Tags[11]	中间人攻击 重放攻击 恶意代码注入	较高	可识别系统	是	集中式	$O(1)$	能
轨迹分析	ACD[1]	未增强原系统抵御攻击的能力	在大型系统中下,ACD 检测准确率达 71.53%	可识别系统	否(对于各种数据信息的依赖太大)	集中式	$O(n^3)$ Floyd 算法	否
	DeClone(Feng)[12]	未增强原系统抵御攻击的能力	在大型系统中,DeClone 检测准确率可达 88.24%	可识别系统	否(对于各种数据信息的依赖太大)	集中式	$O(n^2)$ Dijkstra 算法	否
	基于 RFID 的供应链多维防伪异常监控模型[13-14]	窃听攻击	正确率最高可达到 99% 且误检率低	可识别系统	否(对于各种数据信息的依赖太大)	集中式	由于该模型进行多维异常检测,故时间花销比较大	能
	基于 RFID 供应链的双轨迹克隆检测方法[15]	重放攻击	高	可识别系统	是(不依赖于任何预先定义的供应链结构或正确的产品信息流)	集中式	标签不执行任何计算,阅读器只进行了轻量级的操作	否
碰撞检测	BASE[20]	易遭受窃听攻击	64%	匿名系统	是	集中式	$O(n)$	否
	DeClone(Bu)[20]	易遭受窃听攻击	77%	匿名系统	是	集中式	$O(n)$	否
	DeClone+[20]	易遭受窃听攻击	较高(且可以调节)	匿名系统	是	集中式	$O(n)$	否
	基于多种子的大规模 RFID 系统概率性克隆攻击识别方法[19]	易遭受窃听攻击	较高(且可以调节)	匿名系统	是	集中式	$O(n)$	否
	MT-CAI[21]	未增强原系统抵御攻击的能力	最高可达 100%	可识别系统	是	集中式	$\Theta(n)$	否
	CAIP[16]	未增强原系统抵御攻击的能力	高	可识别系统	是	集中式	$O(n)$ 算法在系统的吞吐率和执行时间上明显优于其他算法	能
	Clone tag detection in distributed RFID systems[22]	未增强原系统抵御攻击的能力	99%	可识别系统	是	分布式	$O(n*d)$ (d 是成对独立的散列函数个数)	能

对表 1 进行分析可以发现,现有的克隆标签检测方法大多具有以下两个特点:(1)基于可识别 RFID 系统;(2)采用集中式检测。

可识别 RFID 系统允许使用标签 ID 进行克隆检测,即在检测前相关的标签 ID 信息(包括 ID 基数)是能够被获取到的。但是基于可识别 RFID 系统不利于隐私保护,后端服务器与读写器之间或读写器与标签之间的标签 ID 通信存在 ID 泄露的风险。例如,考虑一个军事射频识别系统[23],标签 ID 可以显示武器的类别,而 ID 基数可以确切地显示武器的数量。如果采用可识别 RFID 系统,则可能通过标签 ID 和 ID 基数暴露军事实力。而匿名 RFID 系统就像一个“黑盒”,阅读器无法从标签或后端服务器查询标签 ID,同时匿名 RFID 系统也对隐私敏感的应用程序进行了保护。所以,考虑到对于隐私的保护,研究匿名 RFID 系统很有必要。

然而,这样严格的要求使得像文献[1,12-15]这样依赖 ID 的轨迹分析方法不再适用于匿名 RFID 系统,这些方法需要从供应链或者生产商那里收集 ID 信息,并在一个 ID 同时出现在不同地方时检测到克隆攻击。

此外,表格中的方法几乎都是集中式检测,克隆标签和它对应的真实标签要求在同一系统中被检测,有的甚至要求克隆标签与真实标签必须出现在同一时间同一地点,这就使得这种方法的应用场景较为单一,适用于类似于展览会这样克隆标签与真实标签共存且标签经常被读取的场景,而分布式即阅读器可以基于标签中的某些共享秘密独立检测克隆标签,无需求助于所有标签的全局知识。

因而,为了兼顾隐私性和适用性,研究匿名 RFID 系统的克隆标签检测是必须的,而分布式检测方法是值得去努力的。当然,这是一个富有挑战的事。根据前面的分析来看,想要实现匿名 RFID 系统克隆标签的分布式检测,像轨迹分析这类方法似乎不太可行了,很难应用到匿名 RFID 系统中去。而通过文献[16,19-22]可以发现碰撞检测既适用于可识别 RFID 系统又适用于匿名 RFID 系统,所以后续对于匿名 RFID 系统克隆标签的分布式检测研究,可以重点去研究碰撞检测这一类方法。

同时需要注意的是,RFID 系统克隆标签的分布式检测或许无法通过碰撞检测这一类方法完美地解决,因为就目前的方法来看,针对匿名 RFID 系统还只能检测到存在克隆标签,而无法区分克隆标签与真实标签,可能需要后续通过人工干预的方法,或与其他技术相结合,如先进的外观防伪和射频指纹识别技术来进行辨别。

3　结束语

对 RFID 克隆标签检测领域的一些方法进行了研究,并将现有检测方法分为了射频指纹、同步秘密、轨迹分析和碰撞检测四大类。就目前的研究成果而言,以上四类检测方法均存在不足之处。基于物理层的射频指纹需要借助其他设备进行信息采集,以获取 RFID 标签的物理层射频信息,无法实时检测。同步秘密和碰撞检测方法需要修改 mac 层协议或重新设计软件,并且碰撞检测要求克隆标签与正版标签出现在同一时空。而基于轨迹的检测方法则可能受到数据的限制,供应链合作伙伴可能出于隐私考虑而不共享数据跟踪,缺乏完整的数据追踪将会阻碍克隆检测。相较于可识别 RFID 系统,匿名 RFID 系统有更好的隐私性。但是经过对比分析发现像轨迹分析这类依赖标签 ID 的方法很难应用于匿名 RFID 系统,而像碰撞检测这类方法则既适用可识别 RFID 系统又适用于匿名 RFID 系统。故碰撞检测方法可能会成为今后研究的一个热点。另外,考虑到集中式检测对于检测条件有诸多限制,而分布式则适用性更好。故在之后的研究中匿名 RFID 系统克隆标签的分布式检测是需要努力的一个方向。

参考文献:

[1] HUANG Weiqing, ZHANG Yanfang, FENG Yue. ACD: an adaptable approach for RFID cloning attack detection[J]. Sensors, 2020, 20(8): 2378-2394.

[2] BU K, WENG M, ZHENG Y, et al. You can clone but you cannot hide: a survey of clone prevention and detection for RFID[J]. IEEE Communications Surveys & Tutorials, 2017, 19(3): 1682-1700.

[3] 邱永哲. RFID 标签抗克隆攻击研究现状[J]. 信息与电脑, 2018(5): 121-124.

[4] 张　圳. 基于 RFID 的防伪关键技术研究[D]. 成都: 电子科技大学, 2010.

[5] 沈　帅. 基于 RFID 的轻量级双向安全认证协议研究[D]. 桂林: 桂林理工大学, 2019.

[6] KAMALUDIN H, MAHDIN H, ABAWAJY J H. Clone tag detection in distributed RFID systems[J]. PloS ONE, 2018, 13(3): e0193951.

[7] CHEN X, LIU J, WANG X, et al. Combating tag cloning with COTS RFID devices[C]//2018 15th annual IEEE international conference on sensing, communication, and networking (SECON). Hong Kong: IEEE, 2018: 1-9.

[8] 杨黎斌, 何清林, 罗　冰, 等. 一种快速克隆 RFID 标签检测方法[D]. 西安: 西北工业大学, 2020.

[9] 张国柱, 夏鲁宁, 贾世杰, 等. “牵星”法: 一种基于射频指纹的高频 RFID 克隆卡检测方法[J]. 信息安全学报, 2017, 2(2): 33-47.

[10] LEHTONEN M, OSTOJIC D, ILIC A, et al. Securing RFID systems by detecting tag cloning[C]//International conference on pervasive computing. Nara: Springer, 2009: 291 - 308.
[11] OKPARA S. Detecting cloning attack in low - cost passive RFID tags[J]. An Analytic Comparison between KILL Passwords and Synchronized Secrets Obinna, 2015, 7(1): 1-5.
[12] FENG Yue, HUANG Weiqing, WANG Siye, et al. Detection of RFID cloning attacks: A spatiotemporal trajectory data stream-based practical approach[J]. Computer Networks, 2021, 189: 107922.
[13] 罗梦洁. 基于 RFID 的供应链多维防伪异常监控模型[D]. 海口: 海南大学, 2020.
[14] LUO Mengjie, YAO Xiaoming, LI Chaoran. Multi-dimensional anti-counterfeiting anomaly monitoring model based on RFID in supply chain[C]//Proceedings of 2019 international conference on power, energy, environment and material science (PEEMS 2019). [s. l.]: Advanced Science and Technology Application Research Center, 2019: 5.
[15] 李 香, 刘宴兵. 基于 RFID 供应链的双轨迹克隆检测方法[J]. 重庆邮电大学学报: 自然科学版, 2015, 27(1): 111-116.
[16] 冯 丁. 大规模 RFID 系统中快速识别克隆标签算法研究[D]. 太原: 太原理工大学, 2014.
[17] BU K, LIU X, XIAO B. Approaching the time lower bound on cloned-tag identification for large RFID systems[J]. Ad Hoc Networks, 2014, 13(PT. B): 271-281.
[18] BU Kai, LIU Xuan, XIAO Bin. Fast cloned-tag identification protocols for large-scale RFID systems[C]//2012 IEEE 20th international workshop on quality of service. Coimbra: IEEE, 2012: 1-4.
[19] 陈鸿龙, 艾 欣, 林 凯, 等. 基于多种子的大规模 RFID 系统概率性克隆攻击识别方法: CN110378157A[P]. 2019-10-25.
[20] BU K, XU M, LIU X, et al. Deterministic detection of cloning attacks for anonymous RFID systems[J]. IEEE Transactions on Industrial Informatics, 2015, 11(6): 1255-1266.
[21] 郭奕旻, 李顺东. 基于多叉树的 RFID 克隆攻击快速检测[J]. 计算机应用研究, 2015, 32(4): 1123-1126.
[22] KAMALUDIN H, MAHDIN H, ABAWAJY J H. Clone tag detection in distributed RFID systems[J]. PloS ONE, 2018, 13(3): e0193951.
[23] BU K, LIU X, LUO J, et al. Unreconciled collisions uncover cloning attacks in anonymous RFID systems[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(3): 429-439.

(上接第 109 页)

Inc, 2011: 361-369.
[10] CHAUDHURI K, MONTELEONI C, SARWATE A D. Differentially private empirical risk minimization[J]. Journal of Machine Learning Research, 2011(12): 1069-1109.
[11] CHANDRASEKARAN K, THALER J, ULLMAN J, et al. Faster private release of marginals on small databases[C]//Proceedings of the 5th conference on innovations in theoretical computer science. New York, NY, USA: ACM, 2014: 387-402.
[12] ZHANG J, ZHANG Z, XIAO Z, et al. Functional mechanism: regression analysis under differential privacy[J]. Proceedings of the VLDB Endowment, 2012, 5(11): 1364-1375.
[13] GONG M, PAN K, XIE Y. Differential privacy preservation in regression analysis based on relevance[J]. Knowledge-Based Systems, 2019, 173: 140-149.
[14] 郑 剑, 邹鸿珍. 差异化隐私预算分配的线性回归分析算法[J]. 计算机应用与软件, 2016, 33(3): 275-278.
[15] WANG Y, SI C, WU X. Regression model fitting under differential privacy and model inversion attack[C]//Proceedings of the 24th international joint conference on artificial intelligence. Buenos Aires, Argentina: IEEE, 2015: 1003-1009.
[16] 高志强, 王宇涛. 差分隐私技术研究进展[J]. 通信学报, 2017, 38(A01): 151-155.
[17] KARTAL H, LIU X, LI X B. Differential privacy for the vast majority[J]. ACM Transactions on Management Information Systems, 2019, 10: 1-15.
[18] HUANG H, ZHANG Z, XIAO F, et al. Privacy-preserving approach PBCN in social network with differential privacy[J]. Proceedings of IEEE Trans on Network and Service Management, 2020, 17(2): 931-945.
[19] FREDRIKSON M, LANTZ E, JHA S, et al. Privacy in pharmacogenetics: an end-to-end case study of personalized warfarin dosing[C]//Proceedings of the 23rd USENIX conference on security symposium. [s. l.]: USENIX Association, 2014: 17-32.