RFID协议安全基准测试的漏洞感知图

Shan Chang a, Li Lu b*,*∗, Xiaoqiang Liu a, Hui Song a, Qingsong Yao c  
a School of Computer Science and Technology, Donghua University, 2999 North Renmin Road, Shanghai, 201620, China  
b School of Computer Science & Engineering, University of Electronic Science and Technology of China, No. 4, Section 2, North Jianshe Road,  
Chengdu, 610054, China  
c School of Computer Science and Technology, Xidian University, 2 South Taibai Road, Xi’an, 710071, China

摘要：

RFID系统的安全和隐私问题主要源于RFID标签有限的存储和计算资源以及不可预计的通信环境。尽管已提出了很多关于RFID系统的安全协议，但大多数是有问题的。我们提出一个随机图论方法启用自动基准测试RFID安全。首先，我们将攻击者的攻击能力拆分为一组原子操作。然后，使用VAGs来加强攻击者和RFID系统的联系，其目的是通过一些方法发现潜在攻击者。关于VAGs的定量分析可以预测出攻击者利用潜在缺陷攻击的概率。此外，使用基于联合熵的方法可以测量RFID在被动攻击下的不可分辩性。通过分析和模拟来说明VAGs的正确性和有效性。

1、简介：

RFID是是一种新兴的技术，被用于多种应用，例如：物流业，制造业，零售业，运输业以及防伪等。当攻击对象或者人时，RFID标签可以被用来识别和认证。防止RFID系统泄漏用户的隐私信息，确保系统中的参与者的安全性就显得尤为重要。为此，安全协议被广泛研究以确保数据在阅读器和标签之间传输时的安全性。

RFID标签通常在存储和计算资源上有严格的限制（考虑到成本），这就意味着运用在RFID系统上的安全协议需要轻量，许多常用的加密方法被用于有线系统，例如：基于非对称的密钥，不适合RFID系统。因此，面向RFID的安全协议比那些在有线环境或者其他无线环境中的应用存在更多的缺陷。更糟糕的是，RFID标签的普遍部署环境是开放、不可预知的。一个攻击者可以部署复杂攻击来识破这个协议，提高了RFID系统的威胁性。

为了建立RFID系统的安全模型，一些学者要么提出关于隐私和安全的形式化的定义，要么是关于攻击者的形式化定义。然而，由于现存在的模型是高层和粗粒度的，设计和分析RFID安全协议仍面临着巨大的挑战。根据先前的模型，很难探测到RFID协议确切的缺陷或者基于这些缺陷的攻击。此外，RFID协议的安全和攻击的影响不能被定量分析。事实上，RFID协议的安全分析仍只停留在初级水平上。因此，为安全协议开发自动化分析和标记管理方法对于提高RFID系统的安全性是相当重要的。在这篇文章中，我们提出了随机图论的方法协同细粒度的攻击者模型来自动分析标记RFID安全协议。我们的工作主要来源于五个方面。

第一点，我们提出了一个更为灵活的攻击者模型，细粒度，现实结构。我们形式化攻击者的一组原子操作。通过一些原子操作，攻击者的任何攻击可以被准确的表示。与之前的模型有所不同，我们的模型所定义的原子操作可以更加精准的仿真现实世界中的攻击者。

第二点，为了描述一个攻击者是如何与一个标签或单独一个阅读器产生联系的，我们并没有生成一个单独的状态传输图来表示标签和阅读器之间的关系。我们提出了一个新颖的随机图论方法，叫做VAGs（脆弱性感知图），这个方法用到了一对图:标签图（TG）和阅读器图（RG），分别用来表示攻击者与标签以及攻击者和阅读器之间的联系。VAGs探测安全协议的潜在缺陷和分析对手的攻击模式。通过利用VAGs，一个攻击可以在标签图或者阅读器，图中被映射成一条有害路径。我们设定一组规则定义有害路径。每一条路径代表一个有缺陷的协议。每一条有害路径代表攻击者的一个动作。因此，通过找出有害路径，我们可以派生出攻击模式。

第三，攻击者几乎不能利用极其微笑的缺陷。可以计算出攻击者能探测和使用缺陷的可能性，即，他或她能沿着代表缺陷的路径的概率，我们进一步分析了攻击者可以利用流量和定量攻击的概率。

第四，被动的攻击者不会干扰标签和阅读器之间的通信，他仅仅只给标签的不可辨别性带来了威胁，一个被动的攻击者的VAGs被缩减为一对图像，说明了一对阅读器和标签之间的联系。我们提出另一个基于联合熵的方法来测量被动攻击下，标签的不可辨别性。

最后，我们实现了RFID安全协议的整体基准测试方法。

本文其他部分的组织如下：在第二部分我们讨论了相关工作，第三部分介绍了预备知识，第四部分是攻击模型，第五部分形式化定义了这个问题，VAGs方法在第六部分详细进行了介绍。第七部分讨论了在被动攻击下测量标签的不可区分性。第八部分展示了案例研究，第九部分结束我们的工作。

1. 相关工作

在本节中，我们将简要介绍以前与我们工作密切相关的研究，包括RFID安全模型，基于图的网络安全分析方法，RFID基准测试和RFID协议的安全评估。表1从提出安全模型，安全基准测试，自动协议分析，定量分析和攻击防范类型等几个方面说明了现有工作与提出的工作的不同之处。

2.1 RFID安全模型

一些研究人员正致力于建模RFID系统的安全或隐私[7-11]。A. Juels等人 [9]定义了用于RFID系统基本分析的RFID系统的强大的私密性。 协议是否是强大的私密性可以手动分析。但是，该定义没有提及如何自动分析协议。X.Zhang等人 [7]描述了一些安全要求，包括标签数据的隐私性，所有权的隐私性，标签数据的完整性以及RFID系统中标签身份的可用性。 然后正式确定这些要求的定义。I. Damgard等人 [10]通过指定她可以采取的行动来模拟对手的行为，但是敌手模型对于表征现实对手是粗粒度和不灵活的。 G. Avoine [11]也引入了适用于RFID环境的对手模型。对手的形式化只能用于分析协议的可追溯性。 S.Vaudenay [8]基于文献[9]提出了RFID系统匿名识别的模型和定义。 它考虑了RFID系统中的标签持有相关密钥的情况，并讨论了安全与效率的权衡。。

2.2 基于图形的网络安全分析方法

开发了场景图[12]和攻击图[13]（这是一种特定类型的情景图）来评估网络系统的安全性。利用攻击图和生成攻击图分析网络漏洞已有很多工作[13-16]。攻击图可以显示网络中不同主机上的漏洞之间的关系。它考虑到了由主机之间的交互激活的漏洞之间的相互关系，因为不同主机上的多个漏洞可以一起用来实现某些攻击对象。但是原始攻击图不能充分表达敌手在RFID系统中可能使用的关系。在RFID系统中，攻击者不仅可以利用系统中标签秘密之间的关系（实际上，在许多RFID系统中，对考虑强隐私来说标签是独立的[8]，我们的工作主要集中在这样的RFID系统 ），更重要的是攻击者可以利用在同一标签上的几次协议执行之间的关系，而这些关系不能用攻击图来描述。

2.3 RFID基准测试

还有一些关于RFID基准测试的现有档案[17,18]，但它们主要关注MAC或物理层标签的性能和可靠性。 它们旨在评估周围物体的影响，阅读器的力量，标签与阅读器之间的距离，或标签在标签性能方面的物理取向，如读取速率。

2.4 RFID协议的安全性评估

M. Alizadeh等人 分析了RFID应用中使用的几种轻量级加密算法的安全性（就混淆和扩散而言）。 作者只关注对保密标签的被动攻击[27]。一些研究人员对最近提出的轻量级协议进行了安全和隐私分析，并讨论了它们的优点和安全问题[28,29]。Changshe Ma等人证明ind隐私弱于unp隐私。 RFID标签的必要和充分条件是实现unp隐私性[30]。 伪随机函数族是对RFID标签的计算能力的最低要求，用于执行强大的RFID系统隐私。

表1

现有工作与协议VAGs之间的差异。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 成就 | 安全模型 | 安全基准测试 | 自动协议分析 | 定量分析 | 攻击（被动或主动） |
| [7-11]  [17,18]  [27]  [28,29] | 是  否  否  否 | 否  否  是  是 | 否  否  否  否 | 否  是  是  否 | 两者  无  主动  两者 |
| [30]  VAGs | 是  是 | 是  是 | 否  是 | 否  是 | 两者  两者 |

3、预备知识

3.1 RFID系统

RFID标签分为两个类型：被动和主动标签，他们之间主要的区别是被动标签没有内部能量，但主动标签有，被动标签使用阅读器的射频波作为能量的提供。它因此无法承受复杂的需要相对高功率工作的微处理器。为了降低生产成本，被动标签的存储能力也受到了限制（目前的被动标签一般有千字节的存储）。由于以上硬件的限制，被动标签存在的安全风险是相当高的，被动标签的安全协议比主动标签也存在更多的缺陷。在这篇文章中，我们关注被动标签的安全问题，我们的方法可以协调的应用主动标签的协议。

在RFID系统中，阅读器是用来询问RFID标签的一个设备。对于被动标签，阅读器负责激活标签的微芯片。阅读器没有存储关于标签或者系统的敏感信息。在获得标签的响应后，它简单的传输结果到后台服务器用于进一步加工。一般的，阅读器和后台服务器的信道认为是安全的。标签和阅读器的通信时通过两个开放的未加密的无线信道，即阅读器-标签（正向通道）和标签-阅读器（反向信道）通信。正向通道的通信距离比反向通道大的多，因为阅读器的传输能量比那些标签要大的多。相应的，攻击者在正向信道的窃听距离也比反向信道大的多。后端服务器处理的系统中处理信息，与标签相关，同时也有强大的计算资源。因此，它被认为是一个安全可信的实体，无法被攻击者盗用。这篇文章中，我们把阅读器视为RFID阅读器和后台服务器相结合的单独一个单元。

被动标签和阅读器之间的通信采用问答机制。阅读器先发起询问，在收到回应后，标签计算出结果，即响应，然后发回给阅读器。在阅读器和标签中安全协议的执行也是基于问答机制的。一个成功的协议的执行叫做会话。在这篇文章中，我们将m定义为标签和阅读器的消息传输，si是RFID安全协议的第i个会话，标签j是系统中的第j个标签。RFID标签和阅读器的自动问答机制一个安全隐患，可以被攻击者轻易获取未经授权的RFID数据。因此，RFID安全和隐私越来越重要了。

3.2 RFID系统的安全问题

一个标签显示了被连接的对象类型，甚至唯一的标识该对象。因此，标签携带的信息与对象所有者的机密信息高度相关。考虑一个攻击者目的在于打破一个RFID系统包括隐私，安全和功能。我们的形式化定义如下。

定义1（隐私）： RFID系统的隐私问题来源于两个方面，一个是带RFID标签的数据泄漏，另一个是通过跟踪标签ID用户行为跟踪或者身份识别。

在确保隐私的RFID系统中，需要考虑匿名和不可追踪性。匿名指一个标签的响应与ID和标签没有联系。不可追踪性需要A不能将一个目标标签相应于其他标签区分开（否则A可以追踪这个标签）。事实上，匿名性和不可跟踪性满足不可区分性，因此这篇文章中我们关注不可区分性。

为了确保不可区分性，传输标签的信息应该互不相同或者相关，从不合适的当事人的角度来说，这是有必要的。不可区分性的两个最重要的威胁就是跟踪和活动表。

定义2（安全）：安全关注与RFID系统的标签仿造问题，意思是A不能欺骗阅读器，即，让阅读器接收伪造标签的响应。（这个定义是与[10]中的安全定义一致的）。

安全性值得是确保标签传输的信息没有在响应式进程中或者之后被篡改。它表明数据没有被非法修改或者销毁。RFID响应式进程的安全可以通过转播，重播，信息重建，数据修改/插入攻击达到折衷。

定义3（功能性）:功能性指所有RFID系统提供的所有功能可以被正确地执行。对于RFID系统来说，它有功能保证，攻击者不能干扰它的功能，例如，让一个合法的读卡机拒绝合法标签，反之亦然。

功能性要求当需要时信息可用。RFID系统为了展示功能性，它必须妥善的运作计算机系统，安全控制和通信信道。拒绝服务攻击是最威胁功能性的方式之一，由于他们可以被轻易的部署，却很难抵御。攻击的类型包括被动衰减的RF信号，和主动干扰和中断通信。De-synchronous攻击时另一个具有挑战的威胁，它会造成阅读器拒绝合法标签。

关注以上问题，我们考虑的与传统的CIA(保密性，完整性和可用性)，需求类似，隐私性对应保密性，安全性对应于完整性，功能性对应可用性。

4、攻击模型

在这部分，我们讨论攻击者的行为，构建几个攻击者可能创建的原子操作。然后我们可以对攻击者在应答式进程中，如何在标签和阅读器中进行干预建立模型。

攻击者是一个实体，它尝试阻碍安全性和隐私性，或禁用系统功能。我们假设攻击者知道RFID系统采用的安全方案，即安全协议的规范。不知道标签和阅读器（后台服务器）之间的秘密共享，除非他或她破解了标签。可以通过一些物理攻击破解标签，但是这些物理攻击时有破坏性的，这就意味着标签在破解后已经失效了。由于标签和阅读器的无线通信是开放的，可以获取部分或完整的消息，可以从正向信道或是反向信道，这依赖于的能力。

可以发出各种攻击，例如窃取拦截合法阅读器和标签直接的通信，流氓扫描包括一个恶意的阅读器，该阅读器可以在没有主人允许的情况下读取标签，跟踪，截取，物理攻击，欺骗（复制，交换，转播，重播等），还有DOS攻击。

尽管这些攻击的目的和形式多样，每个攻击的行为可以被解析为一个由原子操作构成的有限集。换句话说，任何攻击都有一系列的原子操作构成。我们可以把那些操作看作一些预言（每个预言可以看作是黑盒理论，这可以解决某些决策问题），可以访问。

定义4(原子操作):一组攻击者可以访问的操作。

.SendToReader(m,si):这个操作形式化定义了一个模型，在一个通过反向信道协议的会话Si中，发送消息m到阅读器。

.SendToTag(m,tagi,si):这个操作形式化定义一个模型，通过正向信道的协议的会话中，发送消息m到标签j。

.ReceiveFromTag(m,tagi,si):这个操作形式化定义一个模型，在反向信协议的会话中，收到来自tagj的消息m。

.ReceiveFromReader(m,si):这个操作定义一个模型，在正向信道协议的会话中，收到来自阅读器的消息m。

.Corrupt(tagj):这个操作形式化定义一个模型， compromising tagj.A能获取tagj当前的秘密，让tag失效，提高所有的原子操作，与标签j一致的都不能再用了。

.SideChannel(tagj ,si):这个操作定义了一个模型，在协议的会话si中，发现tagj的结果。

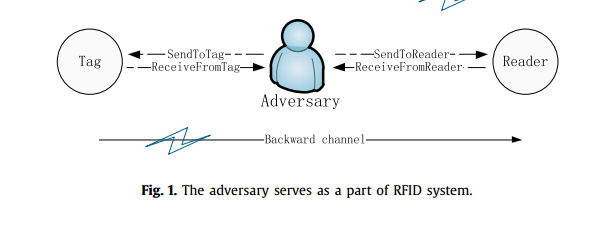


图1.对手是RFID系统的一部分。

的性能是定义4中定义的操作的一个子集。现在我们阐述的性能以及在我们的模型中是如何干扰RFID的。我们把看作是类似于传统的网络中的路由器的中继转发。

.通过访问定义4中的SendTo\*和ReceiveFrom\*操作，能控制所有存在于标签和阅读器（如图一）的通信，决定信息是否是可信，虚假或丢弃（即被拦截）的转播。

.SendToReader和SendToTag操作的通道用来发送消息，该消息遵从阅读器和标签的协议，ReceiveFromReader和ReceiveFromTag代表可以两个信道的传输收到消息。ReceiveFrom∗ 表示，A不仅能窃听在信道传输的消息，也能完全控制这些消息。例如，拦截一条消息代表A用ReceiveFrom的通道，而忽略SendTo\*。

.通过访问Corrupt，可以获取标签中当前的秘密，并通过泄露的秘密和历史信息的观察计算出相应的信息。

.SideChannel允许在给定的会话的获取协议的结果，即接受或者拒绝一个标签。

尤其，上述这些操作不仅可以建立主动也可建立被动攻击者模型，它只监听标签和阅读器之间的通信，并没有以任何方式修改消息流。对于一个被动攻击者来说，他(她)的动作应该遵循以下规则：

.攻击者不能access Corrupt动作

.在会话si中，ReveiveFromReader (m, si) 和 SendToTag (m, tag j, si)需要成对出现。此外，ReveiveFromReader (m, si)也是遵循SendToTag (m, tag j, si)（类似的，ReveiveFromTag (m, tag j, si)也伴随着SendToReader (m, si)），这意味着攻击者如实的传递消息m。

以上的oracle设计展示了我们模型的优点，例如灵活性，细粒度结构，对真实攻击者能力准确的定义。例如，与现存的攻击者模型不同的是，我们的模型解决了把和阅读器（或者标签）的联系变成操作ReceiveFromReader (或者ReceiveFromTag)和SendToReader (或者SendToTag)，以代替将整个联系看作一个单一的动作。类似的，我们应该我们应该把前面用到的ReceiveFrom∗动作拆分为两个更细粒度的动作，ReceiveFromReader和ReceiveFromTag。因此，能访问ReceiveFromReader动作的攻击者也许不能访问ReceiveFromTag，这与现实情况更为接近。这是因为在现实的RFID系统中，窃听范围比扫描范围相对大一些。Tag-to-reader的窃听范围与reader-to-tag的也不相同（前者比后者小）。从另一方面，阅读器与标签也不总是在收到消息后响应，这主要有协议决定。为了反应那些不完全的响应，我们也需要对动作进行更灵活的定义。

1. 问题的制定

在本节中，我们首先描述状态转换模型，分别表示阅读器和，标签和之间的交互。 这对状态转换模型描述了如何介入标签和阅读器之间的通信。 它还描述了标签或阅读器的状态转换如何在发起的操作下进行。然后我们介绍VAGs的正式定义，这是一种随机图形方法，用于RFID安全协议的自动分析和基准测试。

5.1状态转换模型的形式化

我们使用统一的转换系统对由的动作强制形成的标签和阅读器的状态转换进行建模，其中：

1. ：一组状态，
2. ：初始状态
3. :一组转换
4. ：一组最终状态

我们将标签和阅读器视为彼此的对等体。特别的，是具有状态集合的标签状态转换模型。是状态集合的阅读器状态转换模型。接下来，我们专注于和的细节。

• 状态：阅读器（或标签）的状态由其内部状态和外部输出定义。 具体来说，标签和阅读器的状态可以写成如下所示：





• 内部状态（Ins):内部状态包括一组变量，这些变量是只存储在标签（或阅读器）中或与其对应方共享的秘密。 秘密可以是计数器，会话ID，密钥等。注意，尽管在标签或阅读器中存储有不同类型的信息，但对于特定的协议，只有与状态转换相关的信息应该被关注。

• 外部输出：阅读器的外部输出是发送给标签（Chlg）的挑战，而标签的外部输出是对挑战（Resp）的响应。

• （Resp)：Resp表示状态下的标签返回的响应。如果访问SendToTag，那么状态的标签可以通过计算新的Resp为而转移到新的状态，同时将更新为。 可以通过访问ReceiveFromTag来检索。

• （Chlg）：Chlg表示一个由阅读器在生成的挑战。Chlg可以成为读者在会议中主动发起的第一条消息。 对于涉及多个挑战 - 响应交互的协议，Chlg也可以根据访问的SendToReader中的消息m生成。 因此，作为SendToReader的反应，通过准备和将更新为，上的阅读器转移到新的状态。 通过访问ReceiveFromReader接管Chlg。

• 初始状态（Ini）：在交互之前，Ini代表了一个具有原始内部条件的特殊状态。

• 表示从状态到的一个转换。在我们的模型中，如果可以采取SendToTag或Corrupt动作触发标签从到的状态转换，则存在。由于和反映了标签和阅读器之间的交互作用，因此代表标签模型中状态的任何标签响应都必须对应于阅读器模型的至少一次转换。 另一方面，代表阅读器模型中状态的阅读器挑战必须对应于标签模型的至少一次转换。

• 代表由一次Corrupt行为引起的标签的结束状态。 中的标签不能再执行功能。因为永远不会损害阅读器，阅读器不会有这样的状态。

定义5（状态空间的大小）。模型的大小定义为，即其状态空间的大小。

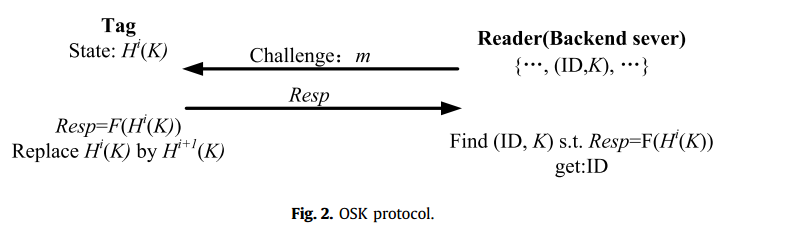


图2.OSK协议

5.2 脆弱性感知图

尽管和描述了RFID系统的每个组件如何在攻击者的行为下响应和更新其状态，但他们仍然不便表达攻击程序。而且，仅用和很难找到所有潜在的攻击。因此，我们开发了一个随机基于图的方法，称为脆弱性感知图（VAGs）。VAGs从三个方面明确描述了状态在和中的相关性：一个会话内一对挑战和响应的因果关系，可能使用的几个会话的相关性，标签和阅读器之间的交互在的存在下。

有很多非等价的方法来定义随机图。 在本文中，我们采用[21]中使用的定义：随机图的形成是一个随机过程，它在描述VAGs的生成方面具有优势。 此外，我们通过允许吊索和有向边来扩展随机图的标准模型。

VAGs包含一对有向随机图，一个反映标签与对手之间的交互作用，称为Tag Graph（TG），另一个反映读者与被称为Reader Graph（RG）的对手之间的交互。 这两个图是根据它们的状态转换模型构建的。TG和RG中的顶点分别表示和中的状态。图中的边表示由SendTo \*或由采取的Crroupt动作引起的状态转换。每个可能的边都以一定概率出现在随机图中。 每个图都有一个没有前导的起始顶点，代表初始状态。

具体而言，对于，每个对应于TG上的一个顶点。对应于从顶点开始并在结束的有向边。是一个没有从它开始的边的顶点。 对于，每个对应于RG上的顶点，R对应于从顶点开始到结束的有向边。

和可以构建为离散时间步长模型以分别创建TG和RG。 VAGs的形成如下：每个图从一个起始顶点（）开始。 在每个时间步中，添加从现有顶点集开始的所有可能边，然后生成尚未创建的边的末端所有对应顶点作为它们的后继。然后这些顶点标记为<内部状态，外部输出>，并添加到现有顶点集中。迭代继续，直到不能添加新的边缘。两个顶点之间的每个有向边表示为进行状态转换所采取的动作。 图中出现边的概率等于可以采取相应动作的概率。

定义6（路径）。表示过渡系统的VAGs中的路径是有限或无限的转换状态序列，该序列连接了一系列状态。

VAGs的目标是自动分析和测试RFID安全协议，检测协议的缺陷并指出潜在的攻击。标签（或阅读器）和之间的任何交互系列可以被视为TG（RG）上的路径。

我们以著名的OSK协议[20]的VAGs作为例子。 OSK协议如图2所示.和都是散列函数。最初,标签具有初始信息,后端服务器存储所有对，对于系统中的每个标签都是不同的。 标签第一次收到来自阅读器的挑战m，它计算，其中是它当前的秘密。 然后它将发送给阅读器，并更新其秘密。 每次遇到挑战时，标签都会重复上述操作。

例如，在会话之后，阅读器发送第（i + 1）个挑战。 在接收到m之后，标签使用其当前秘密（即）计算。 然后，标签发送Resp，即到读取器，并将其秘密更新为。 阅读器从标签接收Resp，并为每个对计算。如果F（H i（K））= Resp，标签将被接受。 请注意，OSK提出了标签操作时间步数的固定上限n。 在第n次询问之后，标签产生随机输出，这是阅读器不能接受的。

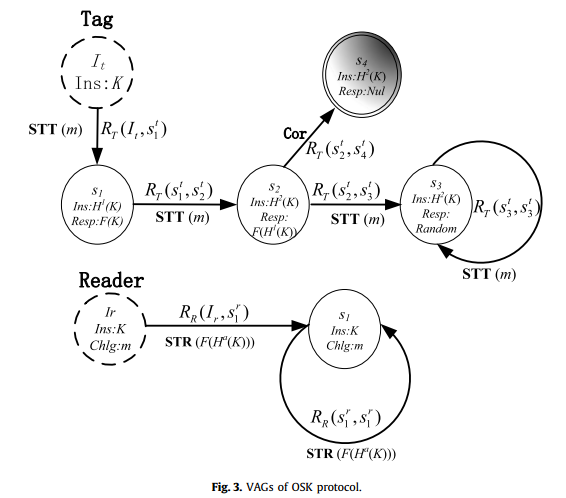


图3.OSK协议的VAGs

1. 脆弱性感知图

我们分别考虑被动和主动的对手。 对于积极的敌手，我们从不可区分性，安全性和功能性角度对RFID安全协议的安全属性进行基准测试。 从图表的角度来看，构成攻击的的行为可以映射到TG或RG上的有害路径。与传统的攻击图或模型不同，我们将安全属性的违规视为某些显示有害特征的路径，而不是检查路径是否会达到某些不安全状态。

在本节中，我们将介绍我们的基准测试方法，该方法可检测RFID协议的潜在缺陷并定义VAGs上的有害路径。 我们还讨论如何量化可以利用这个缺陷发起攻击的概率。 对于被动攻击者来说，它只能对标签的不可分辨性构成威胁。 我们在下一节讨论被动攻击的基准测试方法。

6.1 不可分辨性

不可区分性仅与TG有关，因为它只关注标签的反应与对手的挑战之间的关系。在TG上，可以观察到RFID安全方案的不可区分性取决于TG上是否存在可区分的路径。如果路径上的挑战和响应之间的关系可以被认为是一个特征，那么存在一条可区分的路径。在这里，我们只给出一些可能被攻击者利用的流行特征。实际上，使用我们的模型可以找到更多的特征。

•自循环：TG上的自循环表明存在。这意味着可以采取一些行动使标签返回相同的响应。

•循环：TG上的循环表示存在一系列连续的。以相同的状态开始和结束。这意味着可以采取一些行动来使标签定期返回相同的响应。

定义7（区分路径）。TG上的路径，其上的外部输出（Resps）显示一些特定的特征，例如自循环或循环。

如果在TG上存在可区分的路径，则可以通过执行一系列攻击行为来沿着路径行走，并因此可以观察特征。然后可以根据观察结果区分标签和其他标签。 虽然特征可能是多方面的，但必须注意的是，如果在TG上存在这样的特征，那么应该做的唯一事情就是找到具有特征的路径。由于不同的挑战会导致TG上不同路径所表示的不同响应，为了观察路径的特征，应该在与标签的每次交互中决定挑战（SendToTag中的消息m），以便标签的响应在 根据路径上每个标签状态的响应。因此，我们得出以下结论：

命题1.可以将标签与他人区分的能力被定义为他或她可以在TG上沿着可区分路径选择正确挑战的概率。

6.2 安全

安全意味着不能欺骗阅读器，或者让阅读器接受来自虚构标签的回应。 如果读者接受合法（不妥协）的标签，但标签与阅读器没有匹配的交互，则意味着破坏了RFID系统的安全性。匹配的交互（协议的成功执行）意味着阅读器和标签交换的挑战和响应交织良好，忠实（但可能有一些时间延迟）在会话执行过程中[10]。 我们提出以下定义来描述如果标签和阅读器处于正确执行协议的状态。

定义8（半匹配状态）.假设状态在TG上且状态在RG上，如果与从RG上的开始的转换有关，或者与指向标记图上的转换有关，则这两个状态是半匹配状态，并表示为或。如果至少有一个上述关系是真的，我们说和之间存在一个半匹配。

定义9（匹配状态）.假设TG上的状态满足，并且RG上的满足。这两个状态被定义为匹配状态。 我们说和之间存在匹配。 匹配状态的阅读器和标签意味着它们之间的交互对协议是合法的。

定义10（不匹配状态）.假设TG上的状态和RG上的。如果与指向上的任何转换不相关，与TG上指向t的任何转换都不相关，则和被命名为不匹配状态。如果标签和阅读器处于这种状态，它们不应该在协议的同一个会话中。我们说和是不匹配的。

在发起攻击之前，一对阅读器和标签处于特定的匹配状态。使读者通过伪造合法标签的响应来接受虚构标签。协议的成功执行可以被映射到在VAGs上具有，的几对匹配状态。一般来说，有两种方式来伪造回应。首先，记录由合法标签生成的响应，并在以后直接重播。其次，根据她对系统的了解，猜测一条与真实信息相同的信息。为了获得足够的信息来应对挑战，应找到一条包含TG所需信息的路径。

命题2.给定一个匹配状态，如果A可以从状态找到与有半匹配的TG上的一些路径，即到状态，则可能伪造的响应，并使假冒的回复被阅读者接受。

6.3 功能性

功能意味着协议执行的正确性。由于阅读器功能强大，并且放置在某个安全的地方，因此无法将其分解。然而，会干扰RFID系统的功能，例如，使读者拒绝合法标签或阻止标签识别合法挑战。这意味着能够在TG和RG上执行一系列操作，以便标签无法识别读者，反之亦然，在他们的当前状态。

命题3.攻击从一对匹配状态开始。如果可以在TG或RG上找到路径，以使路径的最终状态为不匹配状态，则在最终状态下功能会崩溃。

有两种方法故意使标签对阅读器无法识别。一种是在TG上从当前半匹配状态找到一些路径到另一个与不匹配的状态。另一种方法是在RG上找到从到状态的一些路径，这是与不匹配的状态。然后，尝试采取沿路径上的有向边表示的一系列动作。如果标签和阅读器之间没有交互发生，阅读器的状态不会改变，而标签的状态通过被驱动到路径的目标状态。

标签拒绝阅读器识别的策略与上述两种方法类似。不同之处在于，在当前状态时，应找到一个路径，其结束状态与RG上的不匹配或与TG上的状态不匹配。

6.4 量

如上所述，隐私，安全和功能方面的缺陷都可以被视为有害的途径。因此，在我们的定量分析中，我们只考虑所有有害路径的统计数据，没有通过缺陷类型来区分路径。 但是，我们的测量也可以用来分析由某种路径表示的某种缺陷。 我们定义了三个用于评估RFID系统安全协议的安全因素：

• 缺陷数量（fn）：由VAGs上的有害路径的数量指示。

• 缺陷的不可感知性（fi）：缺陷可以被利用的概率。

• 缺陷率（for）：在VAGs中有害路径上的状态总数。

必须强调的是，所有这三个因素一起决定了协议的安全性。应全面考虑每个因素对方案安全性的影响。由于所有有害路径都可以位于VAG上，因此我们可以很容易计算出fn和fr。在下面，我们讨论如何计算路径的fi：

所利用的缺陷意味着能够以高概率沿着代表缺陷的有害路径行走。可以通过沿着VAG上的有害路径执行一系列操作来阻碍协议的安全性的概率是：

 （1）

是驱动VAGs上从到的状态转换的概率。它由两个条件概率确定：可以从过渡到的行动的概率，以及可以执行行动的概率。可以执行状态转换的动作的概率定义为可以选择相关的正确消息m的概率。

 （2）

在使用消息m访问STT的条件下，是从到的状态转换概率。它可以从图表中获得一个关于从开始的与m有关的转换的数量。

是选择正确的m并根据从以前的交互中接收到的信息使用它来访问Oracle SendToTag的概率。可以通过访问ReadFromTag（RFT）和ReadFromReader（RFR）来获取信息，以窃听来自阅读器的挑战和来自标签的响应。请注意，获得的消息数量取决于对手的能力。在从标签和阅读器获得消息之后，执行该信息并有可能猜出所需的消息，这取决于先前在特定协议下由标签和阅读器发送的消息的相关性。如果消息之间有很强的相关性，则很有可能猜出所需的消息。

我们给出一个例子来说明如何计算，如图4所示.x，y和z是STT中可能引发状态转换的三条消息。假设他们是独立的，不知道他们，所以猜测每个消息的概率为1/3。从状态开始，x可引起或，y可引起或，并且z可引起RVAG（s1，s3）或。我们计算可以在状态触发某个状态转换的概率如下：







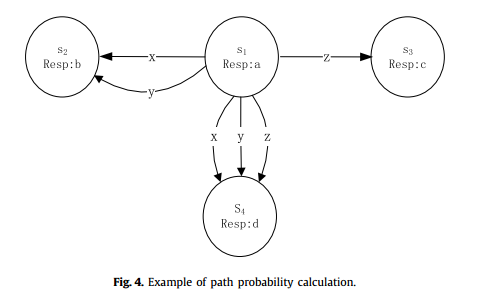


图4.路径概率计算示例

7、在被动攻击中测量标签的不可区分性

由于被动攻击者只是窃听在标签和阅读器间的正向信道和反向信道，这并不会干扰标签和阅读器之间的通信，这只会给标签的不可区分性带来干扰，在这部分，我们阐述了在被动攻击下，如何测量RFID标签的不可区分性。

尽管被动攻击可以通过使用定义4中的原子操作，被很好的形式化定义，被动攻击可以被VAGs准确表示，被动攻击者，本质上，并不采取任何行动迫使标签和阅读器应对假冒挑战。这意味着VAGs将退化成一对图，表示一对阅读器和标签之间的联系。因此，我们提出了另一个方便的方法来测量在被动攻击下标签的不可区分性。

从被动攻击者的角度来看，标签就被看作一个黑盒子，它只知道challenge-responses对，而并不知道它的内部状态。对任何challenge-response机制，我们首先测量了询问和响应的不确定性，和问答对的各自的相互依赖如下。

定义11（不确定的挑战）：标签中，询问C的不确定性是用熵标记，记作H(C),如下：

这里是询问的定义域，c是其中一个询问，p(c)是c出现的可能性。H(C)可以被用来测量攻击者猜测询问的可能性。通过伪造一个合法的询问，攻击者可以获得一个特定的响应。

定义12（响应的不确定性）：响应R的不确定性用熵表示，记作H(R),如下：



是响应的定义域，r是其中一个响应，p(r)代表r出现的概率。H(R)可以被用来测量攻击者猜测到这个响应的可能性。通过假装一个合法的相应，攻击者可以假冒阅读器。

定义13(应答对的相互依赖)：应答对（C,R）的相互依赖是他们之间相互传递的消息。用I(C,R)表示，如下：



p(c,r)是c和r的联合概率分布。I(C,R)用于测量how much a certain challenge tells us about the corresponding response。即，如果我们知道了一个询问，我们能减少多少响应的熵?

于是给了一组标签和阅读器，我们测量标签的不可区分性如下：

定义14（不可区分性）：我们使用联合熵测量问答对（C,R）的不可区分性，记作H(C,R),如下：



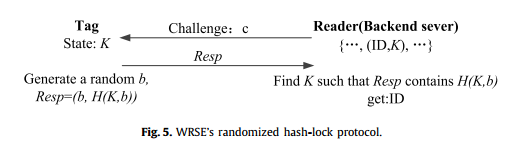


图5.WRSE的随机散列锁协议

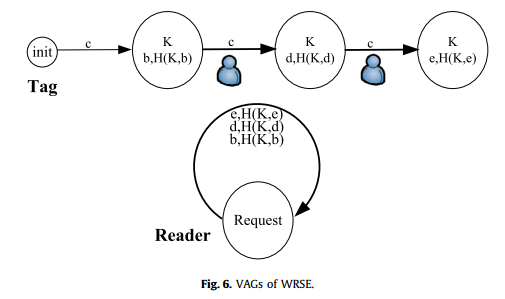


图6.WRSE的VAGs

我们使用联合熵测量在RFID系统中熵含多少，这利用了应答机制。C和R描述相关事件，系统的总熵如下：

*H(C, R)* = *H(C)* + *H(R)* − *I(C, R)*

通过测量一个特定标签的应答对，我们可以评估该标签的不可区分性。在任何RFID系统中，对于一个标签和阅读器对，H(C,R)越大，代表标签的不可区分性越大。

8、基准案例研究

在本节中，我们首先将基准方法应用于WRSE的随机哈希锁定方案[]和OSK协议的变体[8,22]（VOSK），以显示我们方法的正确性和有效性。我们生成WRSE和VOSK的VAGs并呈现我们的分析。安全参数k与状态空间的大小有关。对于RFID系统中使用的实际协议，k应该足够大以保证对手不能通过暴力攻击耗尽所有状态空间。随着k的增加，VAGs的产生将遭遇状态爆炸问题。在本文中，我们的目标不是开发解决状态爆炸问题的方法，而是我们可以使用现有的抽象技术进行模型检查[23,24]，以生成包含一组较小状态的抽象模型，同时保留原始图的安全属性。 我们还可以使用即时技术[25,26]来避免以极小的概率产生可能发生的路径。

8.1 WRSE的随机散列锁协议

我们在图5中说明了WRSE的随机散列锁（WRSE [31]）.H（.）是一个散列函数。每个标签具有秘密信息K，后端服务器存储所有（ID，K）对，对于系统中的每个标签都是不同的。阅读器发送一个持续的挑战c。在接收到c后，标签选择一个随机的k位随机数，并计算H（K，随机数）。 然后它将Resp作为（nonce，H（K，nonce））发送给阅读器。阅读器在所有（ID，K）对中搜索K，使得包含H（K，nonce）。 如果存在这样的K并且拒绝，则阅读器接受标签。

为了给WRSE提供一个直观的印象，我们首先给出一个WRSE的VAGs，其状态空间非常小，如图6所示。我们设置nonce从X = {b，d，e}中选择。在上述参数的设置下，我们描述了WRSE的所有状态和转换。

在图6的TG上，我们使用粗体箭头线来表示可以找到的路径。通过访问RFR获取RG上的挑战c，然后访问STT（c）重复查询标签。因此，可以强制标签将其状态从发送到和，并发起欺骗攻击来破坏系统的安全; 也就是说，可以访问STR来欺骗阅读器接受假标签。

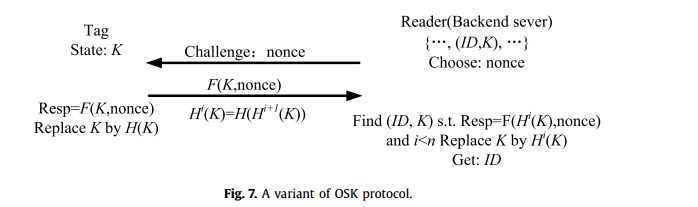


图7. OSK协议的变体

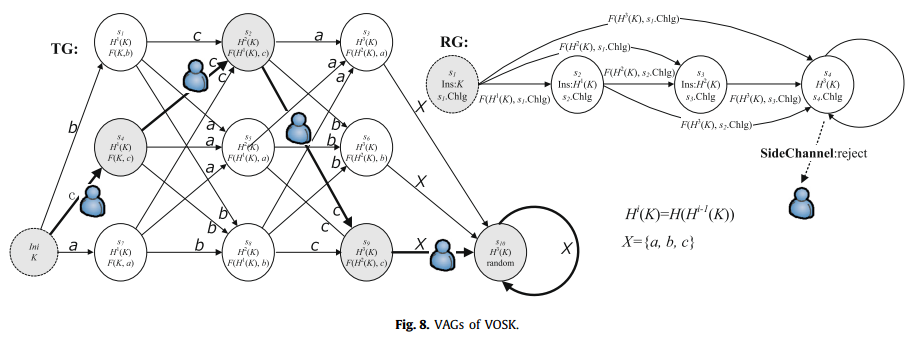


图8.VOSK的VAGs

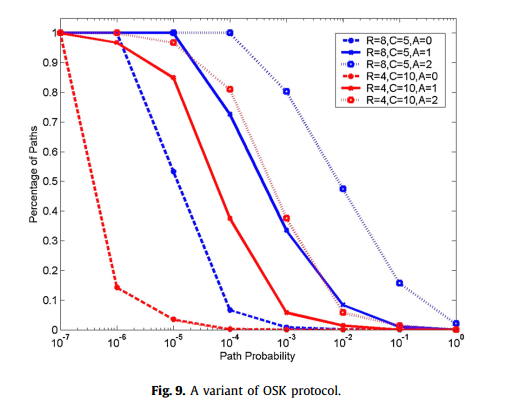


图9.OSK协议的变体

8.2 OSK协议的变体

我们举例说明图7中的VOSK，它与原始的OSK有两个不同。首先，阅读器用随机数（一个随机的α位串）发送挑战。其次，在后端服务器接受标签之后，阅读器更新当前K。

为了给VAGs提供一个直观的印象，我们首先在图8中给出一个具有相当小的状态空间的VOS的VAGs。我们将n设置为4，并且随机数从X = {a，b，c}中选择。在上述参数的设置下，我们描述了VOSK的所有状态和转换。

在图8的TG上，我们使用粗体箭头线来表示A可以找到的路径。通过访问RFR获取RG上的·Chlg，然后访问STT（·Chlg）来重复查询标签。因此，可以找到Ini→→→→的路径，并发起DoS攻击来破坏系统的功能。此外，可以访问SideChannel以了解标签被阅读器拒绝，这也是跟踪的一个可区分特征。

我们设计一个算法来生成VAGs并计算每个路径被找到的概率。图9显示了由我们的算法生成的具有50个状态的VOSK的TG。带有红色实线的路径表示由定位的路径发起DoS攻击。

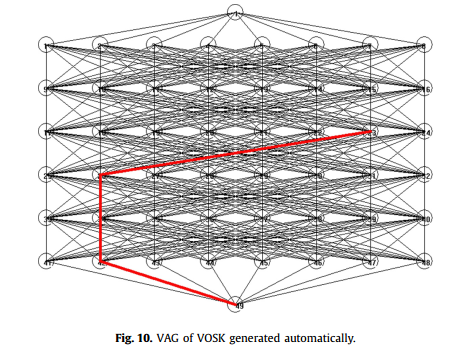


图10.自动生成VOSK的VAGs

在图10中，计算对手定位每条路径的概率，并且在改变状态空间的大小和已有系统的知识数量时，比较不同概率的路径数量。在图8中，R与随机数（α）的长度有关，C表示n的值，表示采取的动作次数。可以看出，在VOSK协议中，一次攻击后，攻击者发起攻击的概率大大增加。还可以看出，在相同的状态空间下，较大的n会导致VOSK协议的安全性较高。

1. 总结

在本文中，我们提出了一种基于随机图的方法来促进RFID安全协议的基准测试和定量评估。该方法包括一个用于表达攻击者能力的细粒度和准确模型，以便攻击者发起的攻击可以被解析为一组原子动作。我们通过对标签和阅读器使用状态转换模型来形式化对手如何干预RFID系统。基于这些模型，我们提出了一种基于随机图的方法VAG，分别反映对手与标签，敌手和读者之间的相互作用。 通过研究有害路径应该具备的特点，我们使用VAG来利用RFID安全协议中的缺陷并分析攻击者的攻击模式。此外，我们讨论对手可以成功发现缺陷并向RFID系统发起攻击的可能性。

参考

[1] R. Oh, J. Park, A development of active monitoring system for intelligent RFID logistics processing environment, in: International Conference on Advanced Language Processing and Web Information Technology, 2008, pp. 358–361.  
[2] Y. Lee, F. Cheng, Y. Leung, Exploring the impact of RFID on supply chain dynamics, in: Conference on Winter Simulation, 2004, pp. 1145–1152.  
[3] M. Bertolini, G. Ferretti, G. Vignali, A. Volpi, Reducing out of stock, shrinkage and overstock through RFID in the fresh food supply chain: evidence  
from an Italian retail pilot, Int. J. RF Technol., Res. Appl. 4 (2013) 107–125.  
[4] H. Hsu, H. Liao, A mobile RFID-based tour system with instant microblogging, J. Comput. Syst. Sci. 77 (4) (2011) 720–727.  
[5] T. Staake, F. Thiesse, E. Fleisch, Extending the EPC network: the potential of RFID in anti-counterfeiting, in: ACM Symposium on Applied Computing,  
2005, pp. 1607–1612.  
[6] J. Jang-Jaccard, S. Nepal, A survey of emerging threats in cybersecurity, J. Comput. Syst. Sci. 80 (5) (2014) 973–993.  
[7] X. Zhang, B. King, Modeling RFID security, in: Conference on Information Security and Cryptology, in: LNCS, vol. 3822, 2005, pp. 75–90.  
[8] S. Vaudenay, On privacy models for RFID, in: ASIACRYPT, in: LNCS, vol. 4833, 2007, pp. 68–87.  
[9] A. Juels, S. Weis, Defining strong privacy for RFID, in: Pervasive Computing and Communications Workshops, 2007, pp. 342–347.  
[10] I. Damgard, M. Pedersen, RFID security: tradeoffs between security and efficiency, in: CT-RSA, 2008.  
[11] G. Avoine, Adversarial model for radio frequency identification, IACR E-print, vol. 49, 2005.  
[12] S. Jha, J. Wing, Survivability analysis of networked systems, in: International Conference on Software Engineering, 2001, pp. 307–317.  
[13] O. Sheyner, Scenario graphs and attack graphs, Thesis, Carnegie Mellon University, 2004.  
[14] P. Ammann, D. Wijesekera, S. Kaushik, Scalable, graph-based network vulnerability analysis, in: ACM Conference on Computer and Communications  
Security, CCS, 2002, pp. 217–224.  
S. Chang et al. / Journal of Computer and System Sciences 81 (2015) 1027–1041 1041  
[15] X. Ou, W. Boyer, M. McQueen, A scalable approach to attack graph generation, in: ACM Conference on Computer and Communications Security, CCS,  
2006, pp. 336–345.  
[16] O. Sheyner, J. Haines, S. Jha, R. Lippmann, J. Wing, Automated generation and analysis of attack graphs, in: IEEE Symposium on Security and Privacy,  
S&P, 2002, pp. 273–284.  
[17] S. Cheung, W. Chan, P. Lee, L. Ni, P. Ng, A combinatorial methodology for RFID benchmarking, in: RFID Academic Convocation, 2006, pp. 1–6.  
[18] M. Buettner, D. Wetherall, An empirical study of UHF RFID performance, in: ACM International Conference on Mobile Computing and Networking,  
Mobicom, 2008, pp. 223–234.  
[19] A. Juels, RFID security and privacy: a research survey, IEEE J. Sel. Areas Commun. 24 (2006) 381–394.  
[20] M. Ohkubo, K. Suzuki, S. Kinoshita, Cryptographic approach to “privacy-friendly” tags, in: RFID Privacy Workshop, 2003.  
[21] P. Erdos, A. Renyi, On the evolution of random graphs, Publ. Math. Inst. Hung. Acad. Sci 5 (1960) 17–61.  
[22] G. Avoine, E. Dysli, P. Oechslin, Reducing time complexity in RFID systems, in: Selected Areas in Cryptography, SAC, 2006, pp. 291–306.  
[23] A. Gupta, Learning abstractions for model checking, Thesis, Carnegie Mellon University, 2002.  
[24] M. Lohrey, S. Maneth, M. Schmidt-Schauß, Parameter reduction and automata evaluation for grammar-compressed trees, J. Comput. Syst. Sci. 78 (5)  
(2012) 1651–1669 (Special Issue: Cloud Computing).  
[25] R. Gerth, D. Peled, M. Vardi, P. Wolper, Simple on-the-fly automatic verification of linear temporal logic, in: International Symposium on Protocol  
Specification, Testing and Verification, PSTV, 1995, pp. 3–18.  
[26] A. Bouajjani, S. Tripakis, S. Yovine, On-the-fly symbolic model checking for real-time systems, in: Real-Time Systems Symposium, RTSS, 1997.  
[27] M. Alizadeh, M. Salleh, M. Zamani, J. Shayan, S. Karamizadeh, Security and performance evaluation of lightweight cryptographic algorithms in RFID, in:  
Recent Researches in Communications and Computers, 2012.  
[28] E. Vahedi, R.K. Ward, I.F. Blake, Security analysis and complexity comparison of some recent lightweight RFID protocols, in: Computational Intelligence  
in Security for Information Systems, CISIS 2011, in: LNCS, vol. 6694, 2011, pp. 92–99.  
[29] B. Niu, H. Li, X. Zhu, C. Lv, Security analysis of some recent authentication protocols for RFID, in: International Conference on Computational Intelligence  
and Security, CIS, 2011, pp. 665–669.  
[30] C. Ni, Y. Li, R. Deng, T. Li, RFID privacy: relation between two notions, minimal condition, and efficient construction, in: ACM conference on Computer  
and Communications Security, CCS, 2009, pp. 54–65.  
[31] S. Weis, S. Sarma, R. Rivest, D. Engels, Security and privacy aspects of low-cost radio frequency identification systems, in: International Conference on  
Security in Pervasive Computing, SPC, in: LNCS, vol. 2802, 2003, pp. 454–469.