供应链环境下安全的RFID通信协议

邓淼磊[1,3] 侯迎春[2] 魏保军[1]
(解放军信息工程大学理学院 郑州 450001)[1] (商丘职业技术学院计算机系 商丘 476000)[2]
(西安电子科技大学计算机学院 西安 710071)[3]

摘 要 射频识别(RFID)技术给供应链管理带来极大的便利。安全的RFID通信协议是实现和保护基于RFID供应链系统安全性的重要方法。描述了供应链环境下RFID通信协议的安全需求,提出了一个新的供应链环境下安全的RFID通信协议。新协议具有较高的效率,且标签端的计算负荷和存储成本较低。

关键词 供应链管理,射频识别,协议,攻击
中图法分类号 TP393.08 **文献标识码** A

Secure RFID Communication Protocol in Supply Chains

DENG Miao-lei[1,3] HOU Ying-chun[2] WEI Bao-jun[1]
(Institute of Science, PLA Information Engineering University, Zhengzhou 450001, China)[1]
(Department of Computer Science, Shangqiu Vocational and Technical College, Shangqiu 476000, China)[2]
(School of Computer, Xidian University, Xi'an 710071, China)[3]

Abstract Radio frequency identification(RFID) technology has greatly facilitated the supply chain management. The application of secure RFID protocols is one important approach for protecting RFID enabled supply chain system. Security requirements for RFID communication protocols in supply chain environments were described. A new secure RFID communication protocol in supply chains was proposed. The new protocol imposes lower computation load and storage cost on RFID tags, and has higher efficiency.

Keywords Supply chain management, Radio frequency identification, Protocol, Attack

射频识别(RFID)技术已经广泛用于工业、农业、商业、军事、交通运输管理等众多行业,尤其应用在企业的多种领域,RFID技术成为企业提高效率、实现管理信息化、增强企业核心竞争力不可缺少的工具和手段[1]。

供应链管理是RFID技术的主要应用领域之一。供应链环境对RFID安全协议提出了一些特殊的安全需求[2]。虽然RFID技术在一般应用中的安全和隐私保护问题已经得到了广泛研究[3-5],但是这些解决方案并不能直接应用到供应链环境中。

文献[2]提出了供应链环境下通信协议需要满足的4个安全需求,并设计了一个能够满足这些安全需求的RFID协议。但是在该方案中,供应链的相邻节点企业需要共享标签秘密,因此无法防止内部攻击。更为严重的是,该方案不能抵抗重发攻击[6]。文献[6]重新定义了文献[2]中的安全需求,并提出了一个通用可组合安全的RFID通信协议,以解决文献[2]中协议存在的安全隐患。但是在文献[6]的协议中,RFID标签需要执行哈希运算。目前,在标签芯片中实现SHA-1等成熟哈希算法大约需要3000到4000个逻辑门。而在供应链中由于标签的使用量巨大,必须将其成本控制在比较低廉的水平,使得RFID标签通常只能拥有大约5000到10000个逻辑门。而且这些逻辑门除了实现一些最基本的标签功能外,仅剩少许可用于实现安全功能。因此,在供应链环境下,需要采用更轻量级的RFID安全协议。此外,文献[7]设计了应用于供应链环境的RFID认证协议,但该协议存在某些缺陷[8]。文献[9]提出了一个易损水印方案,用于对供应链环境下的RFID系统进行篡改检测。

本文在分析供应链环境下RFID通信协议应该满足的安全需求基础上,提出一个新的基于伪随机函数原语实现的RFID通信协议,并对新协议的安全性和效率进行了分析。

1 基于RFID的供应链结构和安全需求

下面描述一个典型的基于RFID的供应链结构和基于RFID的供应链通信协议需要满足的主要安全需求。

1.1 基于RFID的供应链结构

典型的基于RFID的供应链由m个节点企业(P_1,P_2,…,P_m)和一个称作供应链管理中心(VA)的可信机构组成[3]。VA维护一个数据库,并通过有线网络与每个节点连接。每个节点都由相应组织独立管理,它们之间可能互不信任。每个节点都拥有一组RFID读写器(统称为R_i)和一个后端数据库D_i。RFID标签附在物品上。假设供应链中的物流

到稿日期:2010-02-05 返修日期:2010-05-11 本文受国防科技预研项目资助。
邓淼磊(1977-),男,博士生,主要研究方向为安全协议设计和分析,E-mail:dmlei2003@163.com;侯迎春(1973-),男,副教授,主要研究方向为安全协议、无线网络安全;魏保军(1971-),男,博士,副教授,主要研究方向为应用数学。

包括 n 个标签，分别表示为 $T_1, T_2, \cdots, T_n$。物流由 P_1 依次经过 $P_2, \cdots, P_i, \cdots, P_m$。物流到达某个节点后，节点利用RFID读写器从标签中收集产品信息，在处理完毕后将产品交付给下一个节点。

RFID标签成本低、体积小，只有有限的存储和计算能力。标签中只存储少量的诸如产品的ID等信息，产品的详细信息存储在后端数据库中。读写器在收集到标签中产品ID信息后，再通过搜寻后端数据库获得产品的详细信息。本文使用"状态"来描述标签中存储的信息，它是一个 l 位的二进制字符串。为了实现不可追踪性，在处理的不同阶段对于不同的节点需要显示为不同的值。用 T_j^i 表示到达节点 P_i 时的标签 T_j 及它的当前状态，并设 $T^i=\{T_1^i, T_2^i, \cdots, T_n^i\}$。

不失一般性，假设节点企业的读写器与后端数据库间连接是安全的，并把它们视为一个整体；而且后端数据库是不可攻陷的可信实体；而攻击者可以任意地读取、删除、篡改、重发读写器和标签之间的任何消息，也可以在任何时候发起与任一实体的任意会话。这里不考虑对读写器和标签的物理攻击，现有的技术可以很好地防止这类攻击。

1.2 安全需求

供应链环境下RFID协议需要满足以下安全需求[2,6]：

(1)授权访问。预备由节点 P_i 处理的标签只有 P_i 的读写器 R_i 可以访问。也即只有授权的读写器才允许读或更新该标签的状态。

(2)标签认证。只有合法的标签才可以被读写器处理，伪造的标签将不能通过读写器的认证。

(3)前向不可追踪。在某时刻 $\tau'<\tau$，标签 T_j 和某个读写器执行了一轮通信协议；在时刻 τ，攻击者攻陷了该标签，从而获取了标签的当前状态，但是这种情况下攻击者也不能辨别在时刻 $\tau'<\tau$ 时执行协议的实体中是否包括标签 T_j。

(4)标签匿名。攻击者不能够把某个标签的状态同一个随机数进行区分。这主要是为了保护标签的产品信息。

(5)数据重新同步。受到数据同步攻击后，能够使标签和读写器的数据重新同步。

(6)供应链可见性。基于RFID技术的供应链管理最有吸引力的特点就是增强了供应链的可见性。它不需要进行低效的条形码扫描就可以实现对物流处理过程的跟踪和监控。供应链可见性有两方面的含义：(a)供应链的管理者可以对标签进行跟踪；(b)在物流处理的任何阶段，供应链的管理者都能够判断出对标签刚刚进行过处理的是哪个节点。

2 新的RFID通信协议

本节基于伪随机函数原语来设计供应链环境下安全的RFID通信协议。伪随机函数原语可以使用一个伪随机数发生器(PRNG)来实现，而优化的PRNG，只需要不超过1500个门电路[10]。这样的实现代价，对于供应链环境下低成本的RFID标签是合适的。

2.1 系统设置

在方案中，VA负责对所有的RFID标签和读写器进行设置。VA在初始设置阶段就对所有的标签进行设置，而在某节点企业开始处理标签之前才对该节点的读写器(主要是后端数据库)进行设置。在初始设置阶段，VA为每个标签选择一个秘密参数 a_j^1，VA计算 $a_j^i \leftarrow f(r_j \oplus a_j^{i-1})$，其中 $i \in [2, m]$，f 是一个伪随机函数，r_j 是唯一对应于标签 T_j 的随机数，a_j^i 是 T_j 和 R_i 之间共享的秘密数据。VA把记录 $(r_j, a_j^1, a_j^2, \cdots, a_j^m)$ 添加到它的数据库中。

(1)标签的初始设置。在初始设置过程结束之后，标签中存储的数据包括一个序列号、一个初始秘密以及一个更新状态标志位。

(a)标签序列号(r_j)：一个唯一的用来标识标签身份的号码。为了实现标签的匿名性和防止内部攻击，标签只与VA共享该序列号，而各个节点的读写器都不知道该序列号。

(b)标签初始秘密(a_j^1)：一个和读写器 R_1 共享的秘密随机数，用于实现标签和节点企业 P_1 间的双向认证。在成功地执行协议后，该值就会进行更新。

(c)更新状态标志位(u_j)：一位二进制值。$u_j=1$ 表示标签的秘密已经进行了更新，否则 $u_j=0$。

(2)读写器(即后端数据库)的初始设置。每个节点 P_i 都在本地维护一个数据库 D_i，D_i 中包含所有运送到 P_i 的物品信息，其中的每条记录对应于一个标签。对应于某一标签 T_j 的记录包括下列数据：

(a)标签秘密(a_j^i)：用于认证标签 T_j。

(b)指针(p_j)：指向某一网址的字符串信息，与标签有关的商业信息可以从该网址获取。

(c)处理状态标志位(s_j)：一位二进制值。$s_j=1$ 表示相应的标签已经进行过处理，否则 $s_j=0$。

方便起见，用 d_j 表示 R_i 的后端数据库中第 j 条记录 (a_j^i, p_j, s_j)，用 D_i 代表所有记录的集合 $\{d_1, d_2, \cdots, d_n\}$。VA在 R_i 开始处理运送到 P_i 的物流前把数据库 D_i 安全地发送过去。

2.2 协议描述

图1描述了本文设计的节点 P_i 利用读写器 R_i 在后端数据库 D_i 支持下与标签 T_j 进行交互的RFID通信协议，该协议包含了3个子协议(过程)：读协议、写协议和可见性协议。

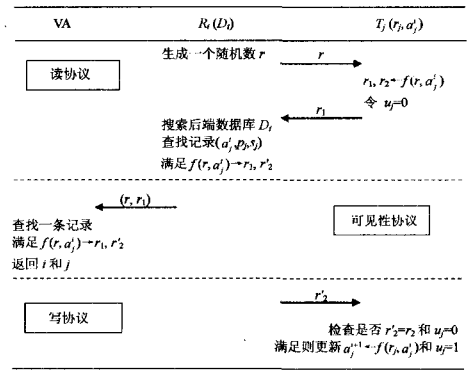

图1 供应链环境下安全的RFID通信协议

(1)读协议。读协议的目标是实现 R_i 从后端数据库 D_i 中查找到 T_j 对应的记录，从而认证标签 T_j。在现实处理中，为了提高处理效率，可以以批处理的方式处理标签。有关批处理技术的详细讨论见文献[2,6]。这里描述的协议仅限于一个读写器 R_i 和一个标签 T_j 的交互。

第一步 读写器→标签：R_i 生成一个非零的随机数 r，把它发送给 T_j。

第二步　标签→读写器：T_j 计算 $r_1, r_2 \leftarrow f(r, a_j^i)$，把 r_1 发送给 R_i。

第三步　读写器认证标签：R_i 搜索后端数据库，查找一条记录 $d_j=(a_j^i, p_j, s_j=0)$，满足 $f(r, a_j^i) \rightarrow r_1, r_2'$。如果不存在这样的记录，那么认证失败；否则 R_i 通过对 T_j 的认证，并可以进一步通过指针 p_j 查询到标签 T_j 的详细信息。

(2)写协议。写协议在节点已经完成了对该标签的所有处理过程之后执行。写协议是为了更新标签的秘密，使得它可以被下一个节点的授权读写器正确处理。并且写协议还可以防止对标签的追踪。

第一步　读写器→标签：R_i 把 r_2' 发送给 T_j，然后设置 $s_j=1$。为了实现可见性，P_i 要向 VA 汇报哪些标签的处理状态标志位已经修改为 1。

第二步　更新标签秘密：接收到 r_2' 后，T_j 检查是否 $r_2'=r_2$ 和 $u_j=0$，如果不满足，T_j 拒绝执行协议；否则，T_j 把 a_j^i 更新为 a_j^{i+1} 并设置 $u_j=1$，这里 $a_j^{i+1} \leftarrow f(r_j, a_j^i)$。

在写协议中，由于只有标签 T_j 和 VA 知道该标签的序列号 r_j，所以只有 T_j 和 VA 能够计算出更新后的该标签秘密。

(3)可见性协议。通过执行可见性协议，VA 可以追踪标签的处理路线，实现可见性。

第一步　读写器→VA：读写器把读协议过程中得到的数据 (r, r_1) 发送给 VA。

第二步　供应链可见性：接收到读写器发来的 (r, r_1) 后，VA 在其数据库中搜索一条记录，满足 $f(r, a_j^i) \rightarrow r_1, r_2'$。然后 VA 返回 i 和 j。

3　安全性和效率分析

3.1　安全性分析

下面分析本文设计的协议能否满足本文第 1 节中描述的各种安全需求。显然，协议的安全性基于标签序列号 r_j 和标签秘密 a_j^i 的安全，所以标签应当具有篡改检测功能[10]。

(1)授权访问。当标签 T_j 运送到节点 P_i 时，一接收到挑战 r，标签就发送 r_1 进行响应，这里 $r_1, r_2 \leftarrow f(r, a_j^i)$。显然，只有掌握标签秘密 a_j^i，读写器才能够计算 $f(r, a_j^i)$ 并检索到正确的记录，从而识别标签。反之，未授权的读写器将不能获得任何有关标签身份的有价值信息。

在写协议过程中，读写器向标签发送 r_2' 作为写命令，只有当 $r_2'=r_2$ 时，标签才执行写协议。根据伪随机函数的性质，只有知道 a_j^i，读写器才能够计算出正确的 r_2，因此只有授权读写器发送的写命令才能被标签接受。

(2)标签认证。在读协议过程中，读写器发送给标签的挑战 r 是一个随机数；因此对于不知道标签秘密 a_j^i 的多项式时间攻击者而言，找到一个合法的响应 r_1，使得 $r_1, r_2' \leftarrow f(r, a_j^i)$ 在计算上是不可行的。因此伪造的标签将不能通过读写器的认证。

这里如果 r 不是一个随机数，读协议就会遭受到克隆攻击。未授权的读写器向一个合法的标签发送 r 后，可以通过复制该标签返回给它的响应来克隆一个标签。此时授权的读写器将不能区分合法标签和克隆的标签。

(3)前向不可追踪。假设攻击者在节点 P_i 攻陷了标签 T_j，从而得到了 a_j^i 和 r_j。但是，攻击者不能够根据 $a_j^i \leftarrow f(r_j, a_j^{i-1})$ 计算出 a_j^{i-1}，因此攻击者不能辨别在节点 P_{i-1} 进行处理的标签中是否包括 T_j。

(4)标签匿名。在方案中，标签只和 VA 共享它的序列号，并且标签返回给读写器的响应和该标签的序列号没有任何关联，匿名性得到了满足。

(5)数据重新同步。在节点 P_{i-1}，如果写协议没能成功执行，那么在 P_i，VA 发送给节点的标签秘密和该标签中存储的秘密将失去同步，从而导致 R_i 不能成功认证标签。一旦出现这种情况，VA 能够通过可见性协议认证该标签，并将该标签的当前秘密 a_j^i 返回给 R_i，实现数据的重新同步。

(6)供应链可见性。VA 知道标签的所有秘密，因此它能够在物流的任何阶段从数据库中找到合法标签的记录，从而识别该标签。一旦 VA 使用某个标签秘密识别了一个标签，它就可以判断出是哪个节点正在处理该标签，因为只有这个节点知道该标签当前的秘密。因此，VA 能够很好地维护供应链的可见性。

3.2　效率分析

下面从存储成本和计算负荷两方面分析协议的效率。

本方案中 RFID 标签只需要存储它的序列号和秘密以及一位更新状态标志，此外标签还需要其他的存储空间用于运算和通信。由于方案中只使用了伪随机函数运算，因此需要的存储空间非常有限。

本方案中标签的计算负荷也较低，标签只需要在读协议和写协议时分别执行一次伪随机函数运算。相比之下，在文献[2]中，标签除了执行哈希运算外，还需要执行异或运算；在文献[6]中，读协议时，标签需要执行一次哈希运算，而在写协议时，标签需要执行两次哈希运算和一次异或运算。在本方案的读协议过程中，与文献[6]类似，读写器需要穷举搜索后端数据库以查找目标标签，运算量较大，不过读写器一般都具有比较强大的存储和计算能力；在写协议过程中，读写器不需要执行任何运算。

结束语　信息采集手段的落后是制约目前供应链管理水平的主要问题之一，RFID 技术在供应链管理中的应用有望从根本上解决这一问题。然而安全性是成功部署基于 RFID 的供应链系统的关键。本文提出的供应链环境下的 RFID 通信协议可以满足授权访问、标签认证、前向不可追踪等安全需求，并且具有较高的效率。

参 考 文 献

[1] 闫新庆，尹周平，熊有伦. 供应链中 RFID 信息的复合访问控制模型[J]. 计算机科学，2008，35(12)：24-27

[2] Li Y J, Ding X H. Protecting RFID communications in supply chains[C]// Proc. of the ACM Symposium on Information, Computer, and Communications Security. Singapore: ACM, 2007: 234-241

[3] 邓淼磊，王玉磊，邱罡，等. 无需后端数据库的 RFID 认证协议[J]. 北京邮电大学学报，2009，32(4)：68-71

[4] Martinez S, Valls M, Roig C, et al. A secure elliptic curve-based RFID protocol[J]. Journal of Computer Science and Technology, 2009, 24(2): 309-318

[5] Burmester M, Le T, Medeiros B, et al. Universally composable RFID identification and authentication protocols [J]. ACM

Transactions on Information and Systems Security, 2009, 12(4): 1-33

[6] 张帆,孙璇,马建峰,等. 供应链环境下通用可组合安全的 RFID 通信协议[J]. 计算机学报,2008,31(10):1754-1767

[7] Juels A, Pappu R, Parno B. Unidirectional key distribution across time and space with applications to rfid security[C]// 17th USENIX Security Symposium. San Jose: ACM, 2008: 75-90

[8] Deursen T, Radomirovic S. Attacks on RFID Protocols [EB/OL]. http://eprint.iacr.org/2008/310.pdf

[9] Han S H, Chu C H. Tamper detection in RFID-enabled supply chains using fragile watermarking[C]// IEEE International Conference on RFID. Las Vegas: IEEE, 2008: 111-117

[10] Coppersmith D, Krawczyk H, Mansour Y. The shrinking generator[C]// Proc. Advances in Cryptology. Berlin: Springer-Verlag, 1994: 22-39

(上接第 33 页)

表 1 主要的互联网应用(包括物联网)的特点

名称	信息形式	信息传输	区别性特征
E-mail	文本	点对点	C/S 结构、非实时
即时通信	文本	点对点	共享屏幕、实时
BBS	文本	公告	文本、讨论
FTP	文件	公告	文件、共享
播客	语音	公告	语音、共享
博客	超文本	公告	HTML、微型 Web
Web	超文本	公告	HTML
语义 Web	超文本	公告	XML、本体
Web 服务	应用程序	公告	WSDL
语义 Web 服务	应用程序	公告	OWL-S、本体
物联网	文本(产品信息)	公告	电子标签、标准化、本体

由表 1 可见,在互联网上所传输的信息,表示形式主要有文本、超文本、文件、语音和应用程序;传输形式主要分为点对点(point to point)和公告(publish)两种。物联网是"文本+公告",与 BBS、博客、Web、语义 Web 的形式相同(在此将超文本视为文本的一种功能增强)。物联网的内在规定性就在于其"文本"的特殊之处。

4.2 物联网之文本的特殊性

物联网之"文本":(1)内容仅限于产品信息。其它互联网应用的文本则可以表达信息提供者想传输的任何信息;(2)内容刻写于电子标签。其它互联网应用是将文本直接输入互联网,物联网则是先通过读取器采集已经刻写在电子标签中的文本信息再将之置于互联网上;(3)内容是标准化的。一方面作为实体的电子标签本身的可利用面积有限,能刻写于其上的文本只能是简洁意骇格式规范即格式标准化,另一方面构成文本内容的词语应是公认通用无歧义的即术语标准化;(4)内容撰写所用词语均源自本体。如同我们撰写文章所用到的每一个字都必须能在标准字典中查得到一样,提交给物联网的产品信息文本中的每一个特征词语都必须存在于至少一个本体之中。这样做,首先是采用了领域内公认的标准词语,其次是基于词语之间的关系机器可以读懂词语的语义。

4.3 物联网归类于语义 Web

在表 1 中,将物联网与其它互联网应用进行比照,与之最为相近的是语义 Web,二者的共同特征是基于本体,相异之处也有着密切的联系:(1)超文本与文本,超文本(hypertext)是含有若干可以进行超链接(hyperlink)词语的文本;(2)XML 与电子标签,XML 是支持信息智能处理的互联网语言,势必成为描述电子标签所载文本的首选;(3)无限定与标准化,标准化只是要遵守一些约定的规范。因为这 3 种联系均是包含关系,故可认为:物联网被归类于语义 Web,是其一种受限定的应用形式。

结束语 词语"物联网(internet of things)"的语义是"物品信息被互联的互联网",其指称的实体为"全球产品信息实时共享系统"。Internet of Things 更恰当的汉译应是"产品信息互联网"。物联网的主性就是"产品信息+互联网",3 个属性则是对这个"产品信息"的具体限定或约束:被刻写在电子标签上;表示格式与所用术语均是标准化的;选用本体中的领域通用词语写成。物联网可视为是语义 Web 的一种应用形式,也就是说,它是在语义 Web 的架构上实现产品信息的智能处理和全球共享。如此归类的意义在于,可以借鉴自 2000 年 T. Berners-Lee 提出语义 Web 构想以来学术界与实业界的研究成果和技术进展,以加速物联网的真正实现。

参 考 文 献

[1] Wikimedia Foundation Inc. Internet of Things: from Wikipedia, the free encyclopedia[EB/OL]. http://en.wikipedia.org/wiki/Internet of things

[2] International Telecommunication Union. ITU internet reports 2005: the internet of things[EB/OL]. http://www.itu.int/internetofthings

[3] 宁焕生,王炳辉. RFID 重大工程与国家物联网[M]. 北京:机械工业出版社,2009

[4] Encyclopedia Britannica Inc. Encyclopedia Britannica[EB/OL]. http://www.britannica.com/EBchecked/topic/592140/thing

[5] 余雷. 基于 RFID 电子标签的物联网物流管理系统[J]. 微计算机信息,2006,22(1/2):233-236

[6] 金岳霖. 知识论[M]. 北京:商务印书馆,2004

[7] 宁焕生,张瑜,刘芳丽,等. 中国物联网信息服务系统研究[J]. 电子学报,2006,34(12A):2514-2517

[8] Urien P, Nyami D, Elrharbi S, et al. HIP tags privacy architecture [A]// Proceedings of 3th International Conference on Systems and Networks Communications (ICSNC)[C]. 2008: 142-147

[9] Urien P, Chabanne H, Bouet M, et al. HIP-based RFID networking architecture[A]// Proceedings of IFIP International Conference on Wireless and Optical Communications Networks (WOCN07)[C]. 2007: 1-5

[10] Auto-ID Center. The Auto-ID Savant specification 1.0 [EB/OL]. http://www.epcglobalinc.org/