供应链环境下安全的RFID认证方案

杨 超[1,2] 张红旗[1,2] 卿梦雨[3]

(解放军信息工程大学 郑州 450004)[1] (河南省信息安全重点实验室 郑州 450004)[2]

(中国人民解放军68202部队 天水 741000)[3]

摘 要 供应链环境下RFID安全认证方案不仅要保证各节点的隐私安全,还应该满足供应链管理需求。针对现有方案存在不能同时兼顾两者的不足,提出一种基于"双重签名"的认证方案。标签的认证信息先后采用访问密钥和认证密钥进行双重签名生成,只有同时具备这两个密钥才能识别标签身份。该方案既可以实现标签在供应链内的安全传递,又能方便供应链的管理。分析表明,该方案较现有方案优势明显。

关键词 供应链管理,射频识别,双重签名,隐私保护

中图法分类号 TP393.08 **文献标识码** A

Security RFID Authentication Scheme in Supply Chains

YANG Chao[1,2] ZHANG Hong-qi[1,2] QING Meng-yu[3]

(PLA Information Engineering University, Zhengzhou 450004, China)[1]

(Henan Province Key Laboratory of Information Security, Zhengzhou 450004, China)[2] (The PLA 68202 Army, Tianshui 741000, China)[3]

Abstract Security RFID authentication scheme in supply chains should not only ensure the privacy and security of all the company, but also satisfy the requirement of supply chains management. Aiming at the problem that existing schemes can't consider both sides at the same time, the paper proposed an authentication scheme based on "double signature". The tag authentication message is signed by the access key and the authentication key. Only possessing both two keys can the company identify the tag. This scheme makes tags transfer safety inside the supply chains and makes the supply chains management convenient. Analysis shows that this scheme has clear advantage compared with existing schemes.

Keywords Supply chains management, Radio frequency identification, Double signature, Privacy protect

1 引言

无线射频识别(Radio Frequency Identification, RFID)技术是一种在开放系统环境中进行对象自动识别的技术[1],最早可以追溯到第二次世界大战期间,美国曾将其用于识别盟军飞机[2]。目前,RFID技术被广泛应用于身份认证、交通管理、军事物流、供应链管理等领域,尤其是供应链管理已成为RFID技术的主要应用领域之一。然而供应链环境的结构特性给RFID安全认证协议提出了一些特殊的安全需求[3]。

供应链由多个既相互独立又相互合作的节点企业组成,每个节点企业都拥有自己的读写器和后端数据库,管理自己所属或所处理的RFID标签。供应链中RFID标签通常被贴在物流的货箱、托盘或者产品上随着物流从一个节点企业到下一个节点企业[4],始终处于不停的流转状态。虽然RFID技术在一般应用中的安全和隐私保护已经得到了广泛研究[1,5-7],但其不能直接应用到供应链环境中。目前常用的RFID标签所有权转换协议[9,10]虽然与供应链环境下RFID技术有些相似,但是它主要考虑标签所有权转换过程中的所有者隐私保护而未考虑对整个供应链系统的管理问题,也不能直接应用到供应链环境中。

本文在分析供应链环境下RFID应该满足的安全需求基础上,提出了一种基于双重签名的RFID认证方案,并设计了实现协议,然后对该方案的安全性进行了分析并与现有技术进行了比较。

2 相关工作

供应链环境下的RFID认证主要考虑的是节点企业的隐私安全及整个供应链的管理问题。下面对现有的几个认证方案进行简要分析。

文献[11]设置了管理中心与所有标签的共享密钥 K_{TTP}。当标签转移发生时,由下一个节点生成新的标签密钥 K_{n+1} 并传给当前节点;由当前节点向管理中心发送当前标签密钥 K_n,提出标签传递请求,管理中心确认后用 K_{TTP} 将 K_n 及 K_{n+1} 加密后通过当前节点传递给标签,标签使用 K_{TTP} 解密验证 K_n 成功后更新标签密钥为 K_{n+1},从而实现标签在节点间流转。因为所有成员节点不知道 K_{TTP},所以该方案可以保证

到稿日期:2013-06-14 返修日期:2013-09-17 本文受国家863计划项目(2009AAZ438),国家973计划项目(2011CB311801)资助。

杨 超(1988—),男,硕士生,主要研究方向为物联网安全,E-mail:ych8988@163.com;张红旗(1962—),男,教授,博士生导师,主要研究方向为等级保护、信任管理、网络安全;卿梦雨(1989—),女,助理工程师,主要研究方向为网络安全。

当前节点的隐私安全，但是 K_{n+1} 是通过当前节点传递给管理中心的，无法保证下一个节点的隐私安全，而且每次都由管理中心参与，管理中心负载太大。

文献[3,12]每个成员节点都保存了当前标签密钥 k_i 及下一个节点的标签密钥 k_{i+1}，标签中存储了当前可访问标签节点的密钥。当标签在节点间传递时，当前节点发送密钥更新消息，将标签内存储的密钥更新为下一个读写器密钥 k_{i+1}，下一个节点便可以直接访问。该协议实质是在两个邻节点间共享了一个密钥，因此两个邻节点间不可避免地会存在隐私泄露问题。另外管理中心无法感知标签的处理状态，无法实现供应链的可见性。

Osaka 等人[13]提出了在两个邻节点间通过临时密钥建立安全信道完成标签转移的方案。方案运行过程中由下一个节点生成一个临时标签密钥 k 并通过安全信道传递给当前节点。两个邻节点通过 k 实现标签传递，下一节点收到标签后再进行密钥更新，实现隐私保护。该方案下一节点更新密钥时必须在一个安全的物理环境中进行，该过程如果遭到窃听，特别是当前节点窃听攻击，便无法保证下一节点的隐私安全。文献[14]提出了一种安全的产生临时密钥及更新标签密钥的方案，从而解决了标签转移过程中前后向隐私安全、标签和读写器假冒及异步攻击等问题。然而该方案无法实现供应链的可见性。

通过分析发现，在供应链环境下现有的 RFID 认证方案都存在以下问题或其中之一：(1)标签流转前后两个节点的隐私泄露问题；(2)文案的设计没有考虑供应链管理问题，无法实现供应链可见。

3 供应链环境下 RFID 安全需求

3.1 供应链环境下 RFID 应用模型

供应链中通常不只一个企业参与，除了主导成员外往往还包含了它的上游成员，如原料供应商、零部件加工商等，以及它的下游成员，如产品批发代理商、零售商等。RFID 标签通常随着物资流动而从一个企业节点移到下一个企业节点，并且供应链成员节点间的直接交互通常仅发生在相邻两个节点之间，因此 RFID 应用可以由图 1 所示模型表示。

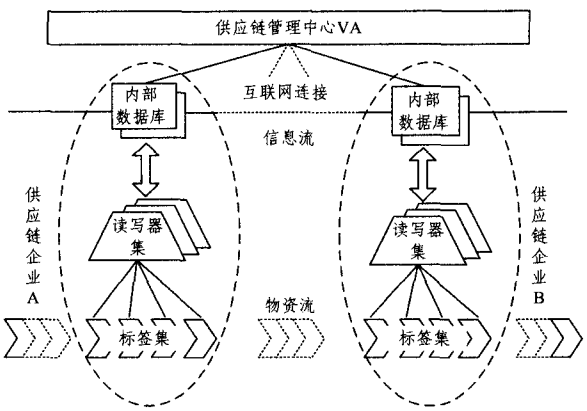

图 1 供应链中 RFID 系统模型

供应链由 m 个成员节点 $P_1, P_2, \cdots, P_m$，以及一个管理中心(简称 VA)组成，每个节点企业 P_i 内部也是一个完整的独立 RFID 应用系统，拥有内部数据库 D_i 及若干 RFID 读写器 R_i。假设供应链中包含 n 个 RFID 标签 $T_1, T_2, \cdots, T_n$。各企业节点与管理中心及节点间通过互联网连接，形成一条信息流，而贴有 RFID 标签的物资则从一个节点到下个节点，形成一条物资流。

当贴有标签的物品到达成员节点 P_i 时，首先 P_i 用自己的读写器 R_i 读取 T_j 的标识信息，然后 P_i 与供应链管理中心 VA 交互获取 T_j 所标识物品的相关信息，进而对其进行相应处理。P_i 对 T_j 处理完之后，根据流程需要可能会更新 T_j 中的信息，并且将需要共享的处理信息发布到 VA 中去，最后 P_i 将处理完毕的标签随物品移交给下一个节点。

3.2 安全需求

供应链环境下 RFID 协议需要满足以下安全需求[3-5]：

(1)授权访问。在将标签 T_j 转交给下一个节点 P_{i+1} 之前，只能由当前处理标签的节点 P_i 读写访问 T_j。

(2)标签认证。只有当前处理节点 P_i 的合法标签 T_i 才能被 P_i 识别，且 P_i 也一定能识别出 T_j。

(3)节点隐私安全。标签 T_j 在节点 P_i 处理完移交出去之后的任何时刻，攻击者都不能通过 T_j 获得有关 P_i 及其处理操作的任何信息。同时在标签传递后不能对下一个节点造成隐私泄露。

(4)标签匿名。攻击者无法将标签的状态同某个随机数区分开。这主要是为了保护标签的产品信息。

(5)可见性。可见性是供应链环境下安全需求的特殊之处，主要是针对管理者而言的，有两方面的含义：1)管理者可以跟踪标签，了解物资流信息；2)无论标签处在哪个处理环节，管理者都可以对标签进行监控。

4 方案描述

4.1 设计思想

一个安全的适用于供应链环境下的 RFID 认证方案既要满足交互前后两个节点的隐私安全，防止攻击者特别是内部恶意节点获得企业节点的隐私信息，又要使管理中心能够对整个供应链进行管理，实时跟踪监控标签处理状态。同时方案还需要满足 RFID 系统其他的安全性和隐私保护需求。根据上述要求，本文提出了一种基于“双重签名”的认证信息生成方式，标签的认证需要同时具备访问密钥和认证密钥，如图 2 所示。

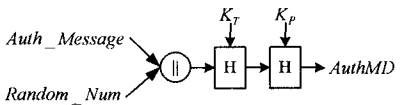

图 2 标签认证信息生成方式

标签的认证信息 $AuthMD$ 需要先后经过访问密钥 K_T 和认证密钥 K_P 签名生成。以 $AuthMD$ 为基础，本文设计了基于“双重签名”的认证方案。该方案可分为 4 个步骤，我们假设标签 T_j 由当前节点 P_i 传递给节点 P_{i+1}，如图 3 所示。

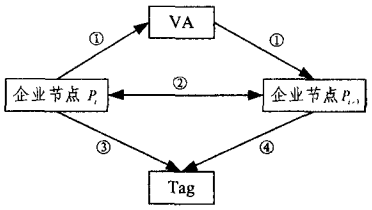

图 3 “双重签名”认证方案

步骤 1 标签传递申请

节点 P_i 处理完标签 T_j 之后向 VA 提出将 T_j 传递给下一个处理节点 P_{i+1} 的申请，T_j 可以是单个标签也可以是标签

集合。VA 经过消息审核确认之后，生成 P_{i+1} 的标签访问密钥并传递给 P_{i+1}，访问密钥由各节点自己保管。为了保证信息交互的安全性，使用了公钥加密系统。各成员节点及 VA 都有自己的公私钥对，公钥是公开的，私钥只有自己知道。一是实现标签 T_j 的处理状态监控，实现供应链可见性，P_i 一旦提出传递申请就代表已经处理完 T_j，并且 P_i 要生成一个关于该申请的数字签名作为不可抵赖的证据。二是实现下一个节点 P_{i+1} 的访问授权，只有经过 VA 授权并获得标签当前访问密钥的节点才能访问标签，从而实现了 VA 对供应链的管理。

步骤 2　信息交换

节点 P_i 将标签 T_j 的唯一标识及标签信息 $info(T_j)$（比如生产日期、地点等）加密传递给 P_{i+1}，同时 P_{i+1} 生成 T_j 的认证密钥并传递给 P_i。一是实现标签信息交换。二是实现 P_{i+1} 的认证密钥传递。认证密钥是由各节点自己生成用于识别各标签的密钥，因为在标签传递前只有 P_i 能够访问标签，所以 P_{i+1} 的认证密钥只能由 P_i 写入标签内部。

步骤 3　密钥更新

完成标签访问密钥及标签认证密钥的更新。最初始的主访问密钥是标签在用于供应链之前由 VA 直接预置到标签内部的，不同的企业节点需要由标签自己在内部按一定的规则更新，实现标签的授权访问。认证密钥则由当前节点 P_i 来更新，P_i 对标签认证确认之后将 P_{i+1} 生成的认证传递给标签，实现标签传递。

步骤 4　标签验证

完成节点 P_{i+1} 通过访问识别标签 T_j 来验证整个标签传递过程是否正确。如果发现不能识别或无法访问，则需要向 VA 请求重新执行该方案。

4.2　系统初始化

假设供应链中的标签都是由 VA 提供的，因此最初信息的初始化是由 VA 直接完成的，如最初的访问密钥预置、最初的认证密钥的分发等。然后标签沿着供应链由一个节点传递到下一个节点。假设参与传递的企业节点是 P_i 和 P_{i+1}，所传递的标签为 T_j，并且标签 T_j 由当前节点 P_i 传递给节点 P_{i+1}。各实体在标签传递前存储的信息情况如下。

VA 存储的信息：

1）T_j，$info(T_j)$：标签的唯一标识 T_j 及标签的其他信息 $info(T_j)$；

2）pk_{VA}，sk_{VA}：VA 的公钥 pk_{VA} 和私钥 sk_{VA}；

3）$\langle ID_i, pk_i\rangle$（$i=1,2,\cdots$）：各企业节点 ID_i 及其相应的公钥 pk_i；

4）K_{T_i}：当前访问节点的标签访问密钥。

P_i 存储的信息：

1）T_j，$info(T_j)$：标签的唯一标识 T_j 及标签的其他信息 $info(T_j)$；

2）pk_i，sk_i：P_i 的公钥 pk_i 和私钥 sk_i；

3）K_{T_i}：节点访问标签的访问密钥；

4）K_{P_i}：节点识别标签的认证密钥；

5）$K_{P_{i+1}}$：节点 P_{i+1} 访问标签的认证密钥，初值为空；

6）$\langle ID_k, pk_k\rangle$（$k=1,2,\cdots$ 且 $k\neq i$）：其他各企业节点 ID_k 及其相应的公钥 pk_k；

7）N：标签密钥更新参数，初值为空。既可用于存放标签更新自己访问密钥使用的参数，也可以存入标签更新下一个节点的访问密钥使用的参数。

P_{i+1} 存储的信息：

1）T_j，$info(T_j)$：标签的唯一标识 T_j 及标签的其他信息 $info(T_j)$，初值均为空；

2）pk_{i+1}，sk_{i+1}：P_{i+1} 的公钥 pk_{i+1} 和私钥 sk_{i+1}；

3）$K_{T_{i+1}}$：节点访问标签的访问密钥，初值为空；

4）$K_{P_{i+1}}$：节点识别标签的认证密钥，初值为空；

5）$K_{P_{i+2}}$：下一个节点访问标签的认证密钥，初值为空；

6）$\langle ID_k, pk_k\rangle$（$k=1,2,\cdots$ 且 $k\neq i+1$）：其他各企业节点 ID_k 及其相应的公钥 pk_k；

7）N：标签密钥更新参数，初值为空。

T_j 存储的信息：

1）K_{T_i}：当前访问节点的标签访问密钥；

2）K_{P_i}：当前节点识别标签的认证密钥；

3）K：标签访问主密钥，由 VA 在最早初始化过程中写入。

4.3　实现协议

该协议主要通过上述 4 个步骤来实现，依次为标签传递申请、信息交换、密钥更新及标签验证。下面协议中以 $E_{pk}(m)$ 表示用公钥 pk 加密消息 m；$H(m)$ 为单向 Hash 函数；Sig_{VA}，Sig_i 分别代表 VA 及各节点用自己的私钥对所发出消息的签名值；N_k 代表各实体生成的随机数。VA 与各节点通过有线网络连接，而各节点与标签则通过无线方式通信。

4.3.1　标签传递申请

协议用公钥加密的方式保障传输消息的安全性，以私钥签名来验证消息的真实性并作为标签传递的不可抵赖凭证。标签传递申请过程如图 4 所示。

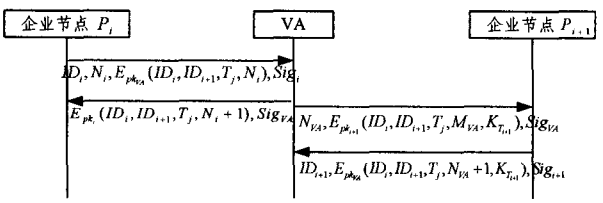

图 4　标签传递申请

1）$P_i \rightarrow VA$：$ID_i, N_i, E_{pk_{VA}}(ID_i, ID_{i+1}, T_j, N_i), Sig_i$

P_i 向 VA 提出标签传递申请，申请消息包括 P_i 的唯一标识 ID_i、P_i 生成的随机数 N_i、用 VA 公钥加密的申请内容和一个用 P_i 私钥生成的消息签名 Sig_i。申请内容需要说明是哪一个标签由什么地方传递到什么地方，因此其中包括 P_i 自身标识 ID_i、传递目的节点标识 ID_{i+1}、传递的对象标识 T_j 以及随机数 N_i。消息签名 Sig_i 既可用于 VA 鉴别消息的真实性，又可以传递申请不可抵赖的依据。

2）$VA \rightarrow P_i$：$E_{pk_i}(ID_i, ID_{i+1}, T_j, N_i+1), Sig_{VA}$

VA 收到申请消息后，通过验证消息的真实性便可以知道 P_i 已经处理完标签 T_j，VA 记录标签 T_j 的处理状态，实现对供应链的管理监控。VA 根据 P_i 的申请内容生成一个用 P_i 公钥加密的申请响应，表示接受该申请，并连同消息数字签名一起回复给 P_i。P_i 收到该回复表示申请得到允许。

3）$VA \rightarrow P_{i+1}$：$N_{VA}, E_{pk_{i+1}}(ID_i, ID_{i+1}, T_j, N_{VA}, K_{T_{i+1}}), Sig_{VA}$

另一方面 VA 为目的节点 P_{i+1} 生成访问密钥 $K_{T_{i+1}}$，并连同本次传递的情况包括标签来源 ID_i、目的节点 ID_{i+1}、所传递的标签 T_j 及随机参数 N_{VA} 用 P_{i+1} 的公钥加密生成接收

标签的通知。VA 然后将生成的 N_{VA}、标签接收通知及 VA 对整个消息的签名值 Sig_{VA} 发送给 P_{i+1}。随机参数 N_{VA} 将作为标签内访问密钥更新的参数用于第 3)步的密钥更新。

4) $P_{i+1} \rightarrow VA$: ID_{i+1}, $E_{pk_{VA}}$ (ID_i, ID_{i+1}, T_j, $N_{VA}+1$, $K_{T_{i+1}}$), Sig_{i+1}

P_{i+1} 接收到 VA 的消息之后，首先根据 VA 签名确认消息的真实性，然后用私钥 sk_{i+1} 解密获得并存储 VA 为自己生成的访问密钥 $K_{T_{i+1}}$ 及参数 N_{VA}，最后根据接收的消息内容生成相应的回复信息并发回给 VA。

4.3.2 信息交换

在标签传递之前，企业节点完成标签信息的共享，同时 P_{i+1} 生成的访问密钥 $K_{P_{i+1}}$ 也需要传给 P_i，为标签中访问密钥更新做准备。同样，交换的信息也用相应公钥进行了加密保护，如图 5 所示。

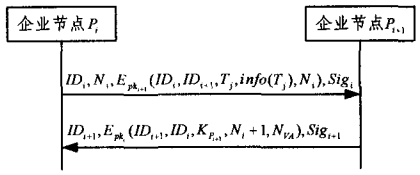

图 5 信息交换

1) $P_i \rightarrow P_{i+1}$: ID_i, N_i, $E_{pk_{i+1}}$ (ID_i, ID_{i+1}, T_j, $info(T_j)$, N_i), Sig_i

P_i 将标签标识 T_j、标签的其他信息 $info(T_j)$ 和自身标识 ID_i 及 P_{i+1} 的标识 ID_{i+1} 用 P_{i+1} 的公钥 pk_{i+1} 加密，并且用自己的私钥生成签名信息 Sig_i，然后一起发送给 P_{i+1}，实现标签信息共享。

2) $P_{i+1} \rightarrow P_i$: ID_{i+1}, E_{pk_i} (ID_{i+1}, ID_i, $K_{P_{i+1}}$, N_i+1, N_{VA}), Sig_{i+1}

P_{i+1} 收到上述消息后，用私钥解密并存储标签标识 T_j 及信息 $info(T_j)$，同时 P_{i+1} 为 T_j 生成自己的认证密钥 $K_{P_{i+1}}$。P_{i+1} 将 $K_{P_{i+1}}$ 及更新参数 N_{VA} 用 P_i 的公钥加密传输给 P_i，P_i 解密并存储 $K_{P_{i+1}}$ 及 N_{VA} 用于下一步的密钥更新。

4.3.3 密钥更新

密钥更新是最重要的一步，只有将标签中的认证密钥及访问密钥都更新为属性 P_{i+1} 的密钥，才能真正地将标签传递给 P_{i+1}。

认证密钥更新

密钥更新之前只有 P_i 能够访问标签，所以认证密钥只能通过 P_i 将 P_{i+1} 生成的认证密钥 $K_{P_{i+1}}$ 写入标签内。认证密钥更新过程如图 6 所示。

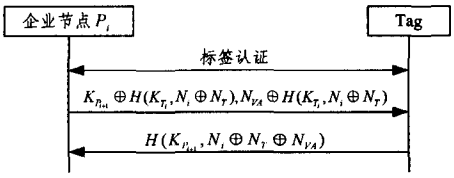

图 6 认证密钥更新

1) $P_i \leftrightarrow Tag$：企业节点 P_i 与 Tag 交互，通过认证协议(见 4.3.4 所示)识别并找出需要传递的标签 Tag。

2) $P_i \rightarrow Tag$: $K_{P_{i+1}} \oplus H(K_{T_i}, N_i \oplus N_T)$, $N_{VA} \oplus H(K_{T_i}, N_i \oplus N_T)$

P_i 收到标签响应后通过查询后端数据库并计算相应的值来识别当前标签的标识 T_j，然后 P_i 确认当前标签是否为需要传递的标签，直到 P_i 找到所需要传递的标签。P_i 用自己的访问密钥加密 $N_i \oplus N_T$ 得到 $H(K_{T_i}, N_i \oplus N_T)$，然后分别将 P_{i+1} 的认证密钥及访问密钥更新参数与 $H(K_{T_i}, N_i \oplus N_T)$ 异或并发送给标签。

3) $Tag \rightarrow P_i$: $H(K_{P_{i+1}}, N_i \oplus N_T \oplus N_{VA})$

标签收到消息 3 后计算 $H(K_{T_i}, N_i \oplus N_T)$ 并解密消息，分别获得 $K_{P_{i+1}}$ 及 N_{VA}。然后标签更新认证密钥为 $K_{P_{i+1}}$，并用 N_{VA} 更新节点访问密钥。

访问密钥更新

节点访问密钥是节点具有标签访问权限的依据，除了 VA 及节点自身外不能让其他节点知道。因此标签内的访问密钥必须通过标签自我更新。

1)我们假设供应链中的标签都由 VA 提供。VA 在将标签引入供应链前为每个标签预置一个标签访问主密钥 K；

2)标签接收到图 6 中消息 3 并获得 N_{VA}，计算 $H(K, N_{VA})$，并以此作为标签当前的访问密钥，即 $K_{T_{i+1}} = H(K, N_{VA})$，完成访问密钥更新。

4.3.4 标签验证

完成前 3 步协议之后，标签 T_j 已经完全传递给 P_{i+1}，标签验证主要是 P_{i+1} 对传递结果的一个确认。

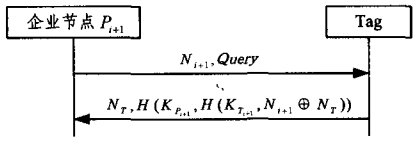

图 7 标签验证

1) $P_{i+1} \rightarrow Tag$: N_{i+1}, Query

P_{i+1} 生成随机数 N_{i+1}，向标签发出访问请求 Query。

2) $Tag \rightarrow P_{i+1}$: N_T, $H(K_{P_{i+1}}, H(K_{T_{i+1}}, N_{i+1} \oplus N_T))$

标签收到访问请求后，同样生成一个随机数 N_T。首先标签以 P_{i+1} 的访问密钥 $K_{T_{i+1}}$ 对 $N_{i+1} \oplus N_T$ 进行第一次签名得到 $H(K_{T_{i+1}}, N_{i+1} \oplus N_T)$，然后以 P_{i+1} 的认证密钥 $K_{P_{i+1}}$ 进行第二次签名得到 $h = H(K_{P_{i+1}}, H(K_{T_{i+1}}, N_{i+1} \oplus N_T))$，最后标签将 N_T 及 h 一起发送给 P_{i+1}。经过双重签名后，只有节点同时具有访问密钥和认证密钥才能识别标签。

3) P_{i+1} 收到标签响应后查询后端数据库并用各标签的访问密钥和认证先后加密 $N_{i+1} \oplus N_T$ 得到 h'，然后比较 $h' == h$ 是否成立。如果能够找到一个满足 $h' == h$ 的标签，则说明传递成功，否则失败，需要请求重新传递。

5 安全性分析

5.1 方案安全性分析

本节将分析该方案是否满足 3.2 节所提出的各种安全需求。每步协议中均使用了公钥加密系统或者单向加密函数，消息传输是安全的，并且每条消息都有一随机数保持新鲜性，各协议能够抵抗窃听、重放等基本攻击，本文在此不作专门分析。

(1)授权访问。标签的访问权限主要通过访问密钥来实现，只有获得当前访问密钥 K_{T_i} 的节点才有机会访问标签。因此保证授权访问的关键集中在 K_{T_i} 的使用及其更新的安全性上。

K_{T_i} 完全由 VA 来分配管理，只有经过 VA 授权的节点才能获得 K_{T_i}，而且当访问权限发生变化时标签内的 K_{T_i} 会更新为新的访问密钥，旧密钥便失效。因此 K_{T_i} 的使用是安全的。K_{T_i} 的更新需要两个参数：主密钥 K 及更新参数。K 由

VA 在将标签引入供应链之前写入，只有 VA 和标签知道，并且任何一个环节 K 都是在 VA 或者标签内部使用，攻击者不可能通过窃听等方式获得，因此 K 是安全的。N_{VA} 虽然要经过 P_i 及 P_{i+1} 传递给标签，但是 N_{VA} 的本质是一个随机数，使用的目的保证标签与 VA 的访问密钥更新一致，同时确保不同节点更新的 K_{T_i} 不同，因此 N_{VA} 不会对 K_{T_i} 更新产生影响。K_{T_i} 更新算法为一个单向 Hash 函数，节点 P_i 不可能从自己的访问密钥中获得任何有关 K 的信息。因此，K_{T_i} 的更新也是安全的。

(2)标签认证。第 4 步协议(第 4.3.4 节)是一次完整的标签访问过程，节点发送的挑战值 N_{i+1} 是一个随机数，合法标签先后用访问密钥 $K_{T_{i+1}}$ 和认证密钥 $K_{P_{i+1}}$ 进行双重签名，并用签名值作为响应。攻击者若不能同时拥有 $K_{T_{i+1}}$ 和 $K_{P_{i+1}}$，找到一个响应 h' 使 $h'==h$，则在计算上是不可行的(等价于破解 Hash 函数)。因此，防止攻击者伪造标签的关键在于保证 $K_{T_{i+1}}$ 和 $K_{P_{i+1}}$ 的安全。

公钥加密系统及单向 Hash 函数的使用，可以保证每步协议消息传输是安全的。除标签外，$K_{T_{i+1}}$ 由 VA 生成，知道它的范围为 VA 和 P_{i+1}；$K_{P_{i+1}}$ 由 P_{i+1} 生成，知道它的范围为 P_i 和 P_{i+1}，即同时知道 $K_{T_{i+1}}$ 和 $K_{P_{i+1}}$ 的实体只有 P_{i+1}。所以，$K_{T_{i+1}}$ 和 $K_{P_{i+1}}$ 是安全的。

(3)节点隐私安全。假设攻击者在节点 P_i 攻陷了标签 T_j，并获得了当前节点的密钥 K_{T_i} 和 K_{P_i}。但是由于 T_j 在传递给 P_i 时 K_{T_i} 是通过单向 Hash 函数进行更新的，且加入了随机参数 N_{VA}；K_{P_i} 是 P_i 重新生成的，所以攻击者不能计算出 $K_{T_{i-1}}$ 和 $K_{P_{i-1}}$，因此攻击者无法辨别 P_{i-1} 是否处理过 T_j，并且不能获得有关 P_{i-1} 的任何信息。虽然 P_{i+1} 的认证密钥是通过 P_i 写入标签的，但是 P_i 仅有认证密钥仍然不能访问标签。P_{i+1} 的隐私能够得到保证。

(4)标签匿名。标签传递申请和信息传递与交换阶段涉及到标签的标识 T_j，但其都用相应公钥加密保护，而密钥更新及标签验证阶段不直接涉及到标签标识，标签匿名性得到保证。

(5)可见性。任何一次标签传递都需要向 VA 提出申请，只有 VA 允许才会给下一个节点生成访问密钥，标签才能进行传递。VA 可以方便地对标签进行管理。VA 根据节点的申请记录可以随时判断出是哪一个节点在处理该标签。因此 VA 可以很好地维护供应链的可见性。

5.2 与现有方案的比较

在相关工作中介绍了现有几种方案的设计思路及其存在的不足，下面在满足安全需求的情况下将本文方案与现有几种方案进行比较，如表 1 所列。其中×代表不满足，√代表满足，△表示部分满足。

表 1 与现有方案的比较

方案	授权访问	标签认证	节点隐私安全	标签匿名	可见性
文献[3]方案	√	√	△	√	×
文献[11]方案	√	√	×	√	√
文献[12]方案	√	√	△	√	×
文献[13]方案	√	√	√	√	×
文献[14]方案	√	×	√	√	×
本文方案	√	√	√	√	√

比较结果显示，本文所提出的方案克服了现有方案存在的攻击弱点，解决了现有方案在供应链可见性管理过程中存在的不足。

结束语 供应链环境下安全的 RFID 认证协议既要能够满足机密性、完整性等基本的传输安全，还要满足企业节点的隐私保护安全，支持供应链管理。本文提出了一种基于“双重签名”的安全认证方案，并设计了相应的实现协议。方案中将标签访问与认证有机分离，由 VA 进行访问密钥的生成、分发，各节点各自生成并维护标签认证密钥，只有同时具备访问密钥和认证密钥才能识别标签身份。通过对协议的分析表明，该协议能够满足供应链环境下 RFID 认证协议的安全需求。与现有方案比较，该方案在安全性及供应链管理方面具有明显优势。

参 考 文 献

[1] 周永彬，冯登国. RFID 安全协议的设计与分析[J]. 计算机学报，2006，29(4)：581-589

[2] Gaukler G M, Seifert R W. Applications of RFID in Supply Chains[M]//Trends in Supply Chain Design and Management: Technologies and Methodologies. London: Springer Verlag, 2007: 29-48

[3] Li Ying-jiu, Ding Xu-hua. Protecting RFID Commu- nication in Supply Chains[C]//Proceeding of the 2nd ACM Symposium on Informatiom, Computer and Communications Security (ASI-ACCS'07). Singapore, 2007: 234-241

[4] 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

[5] 邓淼磊，马建峰，周利华. RFID 匿名认证协议的设计[J]. 通信学报，2009，30(7)：20-26

[6] Lu L, Han J, Hu L, et al. Dynamic key-updating: privacy-preserving authentication for RFID systems[C]//Proceedings of the 5th IEEE International Conference on Pervasive Computing and Communications. New York, USA, 2007: 13-22

[7] 马巧梅，王尚平. 一个超轻量级的 RFID 认证协议[J]. 计算机工程，2012，38(2)：151-158

[8] Fouladgar S, Afifi H. An efficient delegation and transfer of ownership protocol for RFID tags[C]//1st International EURASIP Workshop on RFID Technology. Vienna, Austria, 2007

[9] 陈志德，陈友勤，许力. RFID 标签所有权转换安全协议[J]. 通信学报，2010，31(9A)：202-208

[10] Song B, Mitchell C J. Scalable RFID security protocols supporting tag ownership transfer[J]. Computer Communications, 2011(34): 556-566

[11] Saito J, Imamoto K, Sakurai K. Reassignment scheme of an RFID tag's key for owner transfer[C]//Embedded and Ubiquitouw Computing(EUC). Japan, 2005: 1303-1312

[12] van Deursen T, Radomirovic S. Security of an RFID Protocol for Supply Chains[C]//Proceedings of the 1st Workshop on Advances in RFID, AIR'08. IEEE Computer Society, 2008: 568-573

[13] Osaka K, Takagi T, Yamazaki K, et al. An Efficient and Secure RFID Security Method with Ownership Transfer[J]. Computational Intelligence and Security, 2006, 2(1): 1090-1095

[14] Dimitriou T. RFIDDOT: RFID Delegation and Ownership Transfer made simple[C]//Proceedings of the 4th International Conference on Security and Privacy in Communication Networks. Istanbul, Turkey, 2008: 1-8