一种基于双随机数的 RFID 发现服务安全通信机制

赵 文[1,2],刘学洋[1,2],张世琨[1,2],王立福[1,2]
(1.北京大学软件工程国家工程研究中心,北京 100871;
2.北京大学信息科学技术学院软件研究所高可信软件技术教育部重点实验室,北京 100871)

摘 要: RFID 发现服务没有得到广泛应用,相关标准也没有正式颁布,主要原因之一就是存在诸多安全问题.本文首先分析了存在的典型安全问题,并给出了相应的安全需求,例如 RFID 私密性保护、RFID 编码授权访问、供应链节点不可追踪性、节点认证、消息正确性等.针对这些安全需求,本文提出了一种基于双随机数的 RFID 发现服务安全通信机制.双随机数主要用来对参与通信的双方进行节点认证和消息认证,并给出了相应的查询生成和处理转发流程及算法.本文提出的安全通信机制已经在 PKU RFID^{3}S 系统中得到实现.实验结果表明,系统在实现安全需求的基础上,有较好的查询命中率和查询响应时间.

关键词: RFID; 发现服务; 安全通信机制; 双随机数
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2013)01-0153-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.01.027

A Double Random Number Based Secure Communication Mechanism of RFID Discovery Service

ZHAO Wen[1,2], LIU Xue-yang[1,2], ZHANG Shi-kun[1,2], WANG Li-fu[1,2]
(1. *National Engineering Research Center for Software Engineering, Peking University, Beijing* 100871, *China*;
2. *Key Laboratory of High Confidence Software Technologies (Ministry of Education), School of Electronics Engineering and Computer Science, Peking University, Beijing* 100871, *China*)

Abstract: RFID discovery service is not widely used and related standard is not published, one main reason is the existence of some security issues. Typical security issues are analyzed, and related security requirements are given, i.e. RFID privacy protection, authorized RFID code access, untraceability of supply chain node, node authentication, message correctness, etc. According to these security requirements, a double random number based secure communication mechanism of RFID discovery service is proposed. Random number is used for node authentication and message authentication, and related query generating and routing algorithm are given. This mechanism is implemented in PKU RFID^{3}S system. The simulation tests show that the system not only implements security requirements mentioned above, but also has acceptable query hit rate and query responding time.

Key words: RFID; discovery service; secure communication mechanism; double random number

1 引言

针对大型开环的 RFID 应用,特别是供应链环境下的应用,需要建立跨地区、跨行业的 RFID 公共服务基础设施和信息共享机制,作为核心公共服务之一的 RFID 发现服务,负责收集物品在生命周期内的过程信息,即将分布的物品信息按时间序列整合成完整的物品信息链.

目前对 RFID 发现服务的研究和应用主要集中在安全和性能两个方面:(1) 企业物品信息和供应链信息属于私有信息,需要提供有效的安全通信机制.否则,RFID 发现服务就不可能得到大规模的实际应用,这也正是发现服务相关标准迟迟没有推出的原因之一;(2) 在供应链环境下的大型开环 RFID 应用中,物品数量及物品信息链的数据量十分庞大,服务器过载问题严重.

本文主要研究一种分布式 RFID 发现服务的安全通信机制.通过分析分布式 RFID 发现服务的安全问题,例如,查询过程中消息的防伪造和防篡改、供应链中不同角色能够发起的查询类别应该受到限制、多个供应链中每个节点发起的查询可以到达的位置应该不一样、同一

收稿日期:2011-08-31;修回日期:2011-11-15
基金项目:国家 973 重点基础研究发展计划(No.2009CB320706);国家自然科学基金(No.60803014);"核高基"国家科技重大专项(No.2010ZX01045-001-008)

个节点在不同供应链中可以发起的查询应该不同等,归纳出相应安全需求,例如 RFID 私密性保护、RFID 编码授权访问、供应链节点不可追踪性、节点认证、消息正确性等.基于分布式发现服务的特点,为了满足发现服务查询过程中的安全需求,设计了一种基于双随机数的分布式发现服务安全通信机制,在基于 PKI 对分布式发现服务节点进行认证的基础上,在查询过程中,对 RFID 编码进行哈希以保证其私密性,基于双随机数和哈希算法实现消息的认证.

2 相关研究介绍

2.1 RFID 发现服务

目前,尽管还没有颁布正式的 RFID 发现服务标准,但国内外对 RFID 发现服务解决方案的研究已经形成以下三种模式:

集中式仓库型:这种模式中有一个中央的全局数据仓库,物品在供应链中移动时所产生事件的详细信息不仅存储在企业本地,还要上传到全局数据仓库.尽管这种模式容易实现,但对于海量数据的存储以及提供有效的查询响应是相当困难的;此外,这种模式缺乏私密性保护.

集中式索引型:它是 EPCglobal 提出的一种改进模式,这种模式有一个全局的中央 DS(Discovery Server)[1].当物品在供应链中移动时,供应链各环节产生事件的详细信息存储在企业本地,而本地企业仅将轻量级的事件索引推送给中央 DS.这种模式在一定程度上保护了企业的隐私,并显著降低了中央 DS 存储的信息量,也降低了数据库的查询代价.但这种模式提供的用户接口较为复杂.

跟踪供应链型:这种模式采用分布式结构来代替上述两种模式中的中央服务器.IBM 和微软在从事该模式的研究,研究一种叫做“Theseos”的查询引擎[2].这种查询引擎与 RFID 信息服务[3]绑定.这种模式取消中央 DS,企业的隐私也得到了较好的保护,但查询响应时间较第二种模式长.

文献[4]给出了供应链环境下一种分布式 RFID 发现服务的结构、查询流程等.这种发现服务基于“跟踪供应链”模式,利用 RFID 编码解析服务 NMS(Naming Service,该服务提供根据 RFID 编码查询存储该编码信息的信息服务地址的功能),在发起查询时采用多个查询流以提高查询效率,在返回结果时并行地直接返回给客户端以缩减路由跳数.这种发现服务是本文提出安全通信机制的研究基础.

2.2 安全机制

目前对 RFID 发现服务安全机制的研究主要针对集中式仓储和集中式索引两种模式,而且方法相对单一、简单.

面向集中式仓库型 RFID 发现服务,通过对 EPCglobal 网络中数据流动的分析,文献[5]提出了一种保护集中数据隐私性的方法.在应用层,使用认证和授权技术,提供了三种认证方式,同时也提供了三种授权规则.应用相关规则和技术对数据拥有者进行认证并授权访问.针对 Internet 中的数据通信安全使用 TLS 连接.

系统层的非授权跟踪比传统物理层的危害更大,其结果是全球范围的物品供应链信息被泄露.针对上述情况,文献[6]分析了在集中式索引型半可信 RFID 发现服务环境下非授权跟踪所带来的安全威胁,并提出了一种基于伪标识(Pseudonym)的方法来防止 DS 数据库访问攻击,并提供有效的密钥管理和访问控制.

文献[7]给出了 RFID 发现服务的五个安全需求,即发现服务的选择、信息发布者的控制、访问控制权限的代理、查询的保密性、发现服务的隔离和对等.并针对这些需求,结合两种典型的 RFID 发现服务通信模型(资源目录模型和查询传播模型),讨论了安全需求的实现.特别针对对等,给出了带有安全机制的扁平对等和结构对等模式.最后给出了两种模型的访问控制策略和路由策略.

3 安全需求

在分布式 RFID 发现服务中,基本的查询模式包括三种:Pedigree、Recall 和 Bill-of-Materials[2].在这三种模式中,Pedigree 可以查出物品的所有历史记录,Recall 得到物品当前所在位置,Bill-of-Materials 得到根据物品装箱和拆箱的记录得到包含在一个物品(可能是某种容器,例如集装箱)中的所有物品.除了这三种基本查询以外,可以基于数据库的逻辑模型对其他相关信息进行查询,包括在某个位置的温度等等.

考虑这样一种复杂的供应链场景:一家大型制造企业,通过从多家原材料企业和中间产品企业购买制造产品所需的各类原材料和部件,其中部分中间产品企业需要向更上游的初级产品企业或者原材料企业购买产品;该大型制造企业生产出产品后,需要向各级经销商发货,经过一级经销商、二级经销商、批发商、零售商、大卖场等销售商.由此形成一个以该大型制造企业为核心的供应链.

在上述这样一个复杂的供应链场景中,因为其中的经销商、大卖场、原材料提供商、中间产品企业往往不可能仅仅为一家制造企业服务,他们参与的产品的供应链可能有很多条.

在文献[6,7]以及相关研究中,对供应链的安全需求给出了一些分析.基于这些研究工作,考虑上述分布式 DS 的应用场景,总结得出分布式 DS 中需要考虑的

安全问题如下:

(1)供应链中角色不一,从而能够发起的查询类别应该受到限制.

在供应链中,包括制造商、经销商、零售商、物流企业、最终用户等多个角色,在不同类型的供应链中,这些角色可以进行的查询是不一样的.例如,在药品供应链中,在美国根据法律规定,医院可以根据授权查询其每一瓶药从生产制造到物流中的所有历史信息,以确保病人生命安全;对零售商处于弱势地位的供应链而言,零售商一般不具有进行 Pedigree 查询的权限.

(2)多个供应链并存,每个节点发起的查询可以到达的位置应该不一样.

在多个供应链基于商业关系交织在一起的场景下,每个节点发出的查询,根据查询的类别不同,最终返回的结果可以包含的内容是不一样的.例如,中间产品供应商发起 Recall 查询,要求找到指定的产品现在所处的位置.那么该查询在到达制造企业以后,就应该中止,而不应该继续向供应链下游查找带有该中间产品的最终产品所处的位置.而对于零售商来讲,其进行 Pedigree 查询,也不应回溯到原材料阶段.

(3)同一个节点,在不同供应链中可以发起的查询应该不一样.

对于一些业务比较复杂的企业,其参与的供应链可能有多个,在每个供应链中所处的地位和角色也不一样.相应地,由该节点发起发现服务查询的类型也不一样.在该节点处于优势地位的供应链中,该节点可以发起任意查询;在该节点处于弱势的供应链中,该节点可能只会发出受限制的查询并得到受限制的结果.

(4)查询过程中没有考虑消息的防伪造和防篡改.

在查询过程中,节点之间传输的消息可能会被攻击者截获,并进行篡改或伪造后发送到目的节点,从而破坏发现服务查询结果的正确性.

基于上述分析,给出如下分布式 RFID 发现服务安全需求的描述:

(1) RFID 私密性保护:对于任意一个待查询的 RFID 编码 $Code_i$,对任意 $X\in\{0,1\}^l$,其中 $l=|Code_i|$,都有 $|P_A[D_A(Code_i,X)=1]-1/2|<\varepsilon$,其中 $P_A[]$表示攻击者 A 得到括号中结果的概率,函数 $D_A(Code_i,X)$是攻击者 A 执行任意多项式时间算法,当且仅当它能够区分 $Code_i$ 和 X 时输出 1.

(2)RFID 编码授权访问:对于某个优势企业建立的供应链 SC_y,对于任意的 RFID 编码 $code_i$,如果 $code_i$ 不属于供应链 SC_y,那么对任意的节点 N_x 属于 SC_y,有 $Pr[Query_{Nx}(code_i)=1]<\varepsilon$(当节点 N_x 查询编码 $code_i$ 成功时函数 $Query_{Nx}(code_i)$返回 1,失败返回 0).

(3)供应链节点不可追踪性:对于某个优势企业建立的供应链 SC,那么对任意的节点 N_x 属于 SC,以及任意的节点 N_y 不属于 SC,则 N_y 向 N_x 发起查询并获得结果的概率无穷小,即 $Pr[Query_{Ny}(N_x,Code_i)=1]<\varepsilon$(当节点 N_y 向节点 N_x 查询编码 $Code_i$ 成功时函数 $Query_{Ny}(N_x,Code_i)$返回 1,失败返回 0).

(4)节点认证:对于分布式发现服务中任意一个节点 N_x,当其向另外一个节点 N_y 发出查询请求后,如果攻击者 N_A 假冒 N_y 向 N_x 发送返回信息,则有 $|P_{Nx}[D_{Nx}(N_y,N_A)=1]-1|<\varepsilon$,其中 $P_{Nx}[]$表示节点 N_x 得到括号中结果的概率,$D_{Nx}(N_y,N_A)$是节点 N_x 执行任意多项式时间算法,当且仅当它能够区分 N_y 和 N_A 时输出 1.

(5)消息正确性:对于分布式发现服务中任意一个节点 N_x,当其在查询过程接收到一个消息 M 时,对任意 $X\in\{0,1\}$,都有 $|P_{Nx}[D_{Nx}(M,X)=1]-1|<\varepsilon$,其中 $P_{Nx}[]$表示节点 N_x 得到括号中结果的概率,函数 $D_{Nx}(M,X)$是节点 N_x 执行任意多项式时间算法,当且仅当它能够区分 M 和 X 时输出 1.

4　安全通信机制

分布式发现服务的特点主要包括:并发通信量大、发现服务过程中查询转发次数较多、查询转发与否受限于节点和带有 RFID 标签的物品所属的供应链、查询返回信息传输量相对较小等.

基于分布式发现服务以上特点,为了实现发现服务查询过程中的 RFID 编码私密性保护、节点认证和消息的正确性等安全需求,设计了一种基于双随机数的分布式发现服务安全通信机制.

分布式发现服务安全通信机制在基于 PKI 对分布式发现服务节点进行认证的基础上,在查询过程中,对 RFID 编码进行哈希以保证其私密性,基于双随机数和哈希算法实现消息的认证.在每个节点进行查询的过程中,根据节点类别、RFID 编码和查询类型,确定查询是否被允许和查询是否能够被转发.

在分布式发现服务安全通信机制中,首先应在优势企业或政府管理部门设置一个基于 PKI 的数字证书服务器,负责为每个节点生成并发放服务器数字证书.每个节点加入时,需要分配相应的数字证书,并基于数字证书中的私钥生成节点 ID.数字证书主要用于保证加入分布式发现服务的节点是经过认证的合法节点.

设分布式发现服务由 m 个节点构成(用 $N_1,N_2,\cdots,N_m$ 表示),其中包括 n 个优势企业 $SN_1,SN_2,\cdots,SN_n$.每个节点 N_i 具有唯一的标识 $NodeID_i$,并具有一对公私密钥,其公钥为 KU_i,私钥为 KR_i.H 为一个哈希函

数,节点标识 $NodeID_i = H(KR_i)$.每个节点企业(包括优势企业)N_i 部署一个发现服务引擎 DS_i,每个节点有一个数据库 DB_i,其中存放经过该节点的 RFID 标签编码 $code_j$ 及该编码相关的信息.为了保护 RFID 编码的私密性,实际保存时,RFID 编码 $code_j$ 经哈希后生成 *key* 进行保存.

在分布式发现服务安全通信机制中,涉及到如下几个基本操作:

• $Gen_N(R_N)$:由节点 N 产生一个随机数 R_N.

• $H_N(S)$:由节点 N 对串 S 执行哈希操作,返回值为一个特定长度的二进制串.

• $Verify_{Nx}(CA, N_y)$:节点 N_x 向 CA 验证节点 N_y 的身份,验证通过返回 *true*,验证不通过返回 *false*.

分布式发现服务安全通信机制主要包括两个部分:查询生成安全通信机制和查询转发安全通信机制.下面分别介绍这两个机制的主要步骤.图 1 为分布式发现服务中查询生成安全通信机制.

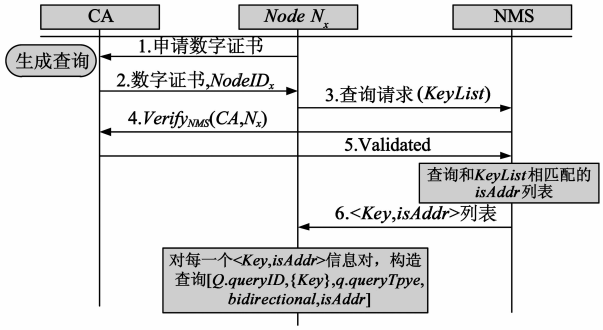

图1 查询生成安全通信机制的主要步骤

查询生成安全通信机制的主要步骤描述如下:

(1)需要加入分布式发现服务的节点 N_x 向 CA 服务器申请数字证书;

(2)CA 服务器在 N_x 身份审核通过后,为 N_x 生成一对公私密钥及数字证书,并基于私钥生成 N_x 的节点标识 $NodeID_x$,并将数字证书和 $NodeID_x$ 发送给节点 N_x;

(3)节点 N_x 向编码解析服务 NMS 发出查询请求,查询内容为待查的 RFID 编码集合;

(4)编码解析服务向 CA 验证 N_x 的身份,如果验证不通过,则结束;

(5)CA 对 N_x 的认证通过,编码解析服务查找和待查询的 RFID 编码列表相对应的 *isAddr* 列表(RFID 信息服务地址列表);

(6)编码解析服务向节点 N_x 返回查询结果,结果为 < *key*, *isAddr* > 信息对的列表;

(7)N_x 基于 < *key*, *isAddr* > 信息对的列表,构造需要对每个 *isAddr* 需要发起的查询,查询消息的内容包括:查询的标识 *queryID*;待查询 RFID 编码对应的 *key*;查询类别 *queryType*(包括 Pedigree、Recall 和 Bill-of-Materials 三种类别);查询方向,以及查询发向的 *isAddr*.

图 2 为分布式发现服务中查询及查询转发的安全通信机制.

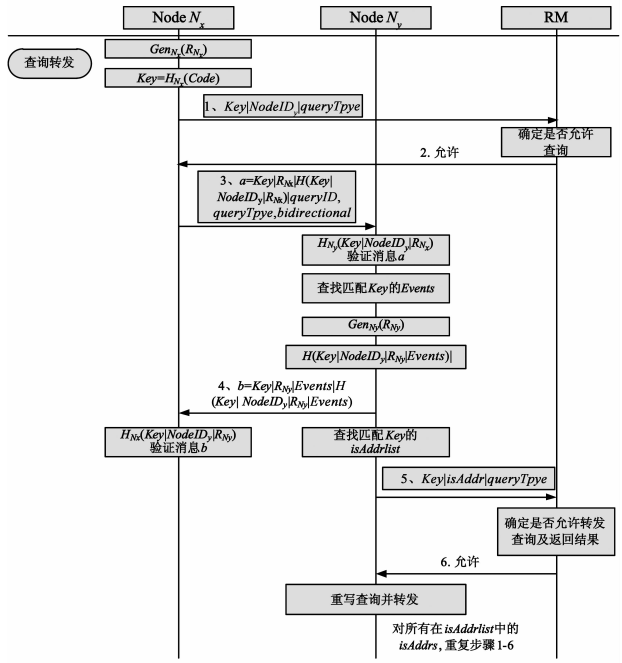

图2 查询转发安全通信机制的主要步骤

查询转发安全通信机制的主要步骤描述如下:

(1)发起查询请求的节点 N_x 产生一个随机数 R_{Nx},并计算待查询 RFID 编码 *Code* 的哈希值 $Key = H_{Nx}(Code)$;

(2)N_x 将查询的 *key*、目标节点标识、查询类别等信息发送到位于优势企业节点上的访问仲裁模块 RM,确定该查询是否允许进行;

(3)访问仲裁模块查询权限数据库中定义的访问控制规则,确定节点 N_x 的此次查询是否允许进行.如果不允许,本次查询终止,否则向节点 N_x 返回查询许可信息;

(4)节点 N_x 获得查询许可后,构造查询请求 $a = Key \mid R_{Nx} \mid H(Key \mid NodeID_y \mid R_{Nx}) \mid queryID$, *queryType*, *bidirectional*(其中"|"表示串连接, *bidirectional* 表明查询在供应链中向上下游两个方向发送),并发向目标节点 N_y;

(5)N_y 用自己的 $NodeID_y$ 计算 $H(Key \mid NodeID_y \mid R_{Nx})$,并用计算结果验证消息 *a* 在传送过程中是否被改变,如果验证不通过,则结束;

(6)N_y 在本地查找和 *key* 对应的 RFID 事件 *Events*,并生成一个随机数 R_{Ny},然后向节点 N_x 发送消息 $b = Key \mid R_{Ny} \mid Events \mid H(Key \mid NodeID_y \mid R_{Ny} \mid Events)$;

(7)N_x 计算 $H(Key \mid NodeID_y \mid R_{Ny} \mid Events)$,并用计算结果验证消息 *b* 在传送过程中是否被改变,如果验证

不通过,则丢弃返回结果;

(8)N_y 在本地查找和 *key* 对应的 *isAddr* 列表,并将待查询的 *key*、查询转发的目标 *isAddr* 和查询类别等信息发送到访问仲裁模块,确定相应的查询转发是否允许进行;

(9)访问仲裁模块接收到查询转发请求后,根据 N_y 节点类型、待转发的目标 RFID 信息服务所在发现服务引擎节点的类型、待查询的 *key*,查询权限数据库中定义的访问控制规则,确定到相应的发现服务引擎节点的查询转发是否允许.如果不允许,则抛弃相应的请求,否则返回查询转发许可信息;

(10)N_y 根据返回查询转发许可信息,对每一个 *isAddr*,重写查询请求,并将查询请求发送到相应的节点.

(11)迭代执行上述步骤直至得到最终结果.

该安全通信机制有效实现了供应链环境下分布式发现服务的安全需求.在该机制执行过程中,节点加入分布式发现服务需要经过 CA 认证,从而保证了非法节点无法进入,同时各节点的标识 *NodeID* 也不会泄漏给攻击者;RFID 编码不会以明文形式出现在通信过程中,从而避免了 RFID 标签私密性的破坏.

当节点收到查询请求后,根据节点类型、待查询编码和查询类型,确定查询是否被允许,从而保证 RFID 编码相关的事件的授权访问.在节点在本地查询中,发现需要进行查询转发时,为了防止供应链内部的信息泄露,根据该节点和待查询编码所在的供应链的优势企业节点确定的安全规则,确定是否允许查询转发,从而确保供应链内部的信息,包括供应链的拓扑结构信息不被外泄.

在节点通信过程中,通过双随机数和哈希函数,实现了发现服务查询通信的双方节点之间的双向认证,确保编码解析返回信息来自于正确的合法节点.通信机制的安全性基于随机数生成程序的安全性和哈希函数的安全性,在上述通信机制中,对参与通信的节点及该节点在本次通信过程中产生的随机数通过安全的哈希函数进行了关联,以实现对该节点在通信过程中的认证.同时,因为产生的随机数使用一次之后即会抛弃,也有效的防范了重放攻击和中间人攻击.在消息传递过程中,通过对传递的消息内容加上节点 ID 进行哈希,实现了对消息内容的认证,能够有效的防止消息篡改.

上述安全通信机制安全性依赖于哈希算法的强度和安全性、访问仲裁模块的安全性以及 PKI 机制中采用密钥长度的安全性,为了保证分布式发现服务安全通信机制的安全性,需要结合实际应用环境,选择合适的算法,并能安全有效地实现访问仲裁模块.

5　算法实现

文献[4]中给出了实现分布式发现服务的若干关键算法,即发起查询、处理并转发、解决查询碰撞、查询结果归并等.下面将安全通信机制加入到相关各算法中,即查询生成算法和查询处理与转发算法,对于不需加入安全通信机制的算法,不包含在本文范围内.

5.1　查询生成算法

在分布式发现服务处理查询的过程中,每个节点的查询引擎首先查询其本地信息服务的相关事件,然后根据本地查询结果生成与其直接上、下游相关的新的查询请求;如果本地查询引擎已经处理过相同的查询,则停止处理.在查询过程中,对于涉及到通信的部分以及需要对节点进行访问仲裁的部分,需要加入相应的安全机制.

为了保证分布式发现服务中节点的合法性,确保加入发现服务网络的节点都是经过认证的节点,需要对合法节点采用数字证书进行认证.在节点加入发现服务前,该节点需要通过数字证书服务器的认证,并得到一对公私密钥 *KU* 和 *KR*,并以其私钥的哈希值设为节点的 *ID*.同时,在每一个优势企业节点建立的供应链中,该优势企业节点需要为该供应链中的查询确定访问控制规则,当节点加入时,需要复制该规则.

在下面的算法描述中,*H* 为哈希函数,*E*(*key*,*S*)表示用密钥 *key* 对 *S* 加密,*D*(*key*,*S*)表示用密钥 *key* 对 *S* 解密,*SendMessage*()的参数按顺序分别为消息目标、消息源、消息内容,其中消息内容包括查询结果、随机数和验证码,*verify_n*()函数向 CA 验证节点身份,*verify_m*()函数验证消息内容的正确性.

算法一:节点 N_x 发起查询的算法

输入:节点 N_x,节点 N_x 的公钥 KU_x 和私钥 KR_x,数字证书服务器 CA,待查询编码列表 *epcList*

输出:转发到和 *epcList* 中 RFID 编码相对应的生产商的查询

```
startQuery(q:Query)
  /* 对待查询的 epcList 中的每个编码,根据发起查询的节点 Nx
  的节点类型、RFID 编码以及查询类型,由本地访问仲裁模块确定
  相应的查询是否允许进行,如果查询不允许进行,则将该编码从
  epcList 中删除 */
  for each epc in q.epcList
    {
      queryCheck(NodeIDNx, epc, q.queryTpye);
      if queryDeny
        q.epcList:= q.epcList-epc
    }
  /* 构造初始查询,其中包含本地发起查询的节点 Nx 的地址,该
```

```
地址将作为被转发的子查询的返回地址.然后向 NMS 查询 epcList 中每个编码对应的生产商的信息服务地址.在 N_x 向 NMS 查询时,NMS 需要向 CA 验证 N_x 的身份 */
starts: = {[q, local]} // q 是初始查询,local 是本地信息服务地址
if not (verify_n(CA, D(KU_x, (E(KR_x, NodeID_x))), KU_x))
    then exit
for each epc in q.epcList
  /* 获的 RFID 编码对应生产商信息服务地址 */
  isAddr: URI: = queryNMS(epc)
  if isAddr ≠ null
/* 为每个 RFID 编码构造一个新查询,其 queryID 与 q 相同 */
    qstart: Query: = [q.queryID, {epc}, q.queryType, bidirectional]
    starts: = starts ∪ {[qstart, isAddr]}
/* 将具有相同信息服务地址的查询合并,以减少查询数量,具体操作是将这些查询的 epcList 都添加到一个查询中,然后删除其它查询 */
starts: = combineByIsAddr(starts)
for each [qstart, isAddr] pair s in starts //并行执行
/* 将 qstart 和初始客户端地址转发到对应的生产商的信息服务地址 */
  processAndRoute(s.qstart, s.isAddr, client)
```

在算法执行完成后,发起查询的节点 N_x 通过向 NMS 查询,获取了和各 RFID 编码对应的生产商的信息服务地址.在向 NMS 查询过程中,需要通过 NMS 安全通信机制[8]以确保查询结果的正确性,并保证查询过程中的 RFID 私密性.同时,在构造查询时,需要在本地根据访问控制规则,确定哪些查询可以进行.

该算法的输出将作为查询处理与转发算法的输入.

5.2 查询处理与转发算法

在生成查询后,由初始发起查询的节点 N_x 向查询得到的各生产商信息服务以及自身的上下游节点发出查询请求,各生产商以及上下游节点在接收到查询后,将根据本地的记录,进行查询并决定是否进行查询转发.在进行查询转发前,需要根据本地节点的节点类型、RFID 编码以及查询类型,由访问仲裁模块确定相应的查询是否允许进行,如果查询不允许进行,则不进行查询转发.各节点在获取查询结果后,将结果直接发送到发起查询的节点 N_x.

算法二:节点 N_x 处理本地查询与转发查询的算法

输入:节点 N_x,查询 q,初始发起查询客户端地址

输出:需要转发的重写后的查询[4];本地查询结果

```
processAndRoute(q: Query, isAddr: URI, client: URI)
  /* 首先检查是否有"查询碰撞"发生,即具有相同查询 ID 的查询是否已经在本节点执行过,如果是,则说明该查询在之前已经被其他节点转发到本节点,算法结束 */
  if checkIfQueriesCollision(q) = true
      exit;
  /* 如果没有"查询碰撞",执行本地查询
  result: Result = queryLocal(q) //在本地信息服务上执行查询 q
  /* 根据本地查询结果,获取与待查询编码相对应的直接上、下游节点集合,并将查询 q 改写为发向这些节点的新查询.在查询发送过程中,需要进行节点认证和消息的认证,节点认证只进行一次,用来建立信赖关系 */
  q_new: Query = rewriteQuery(q, result)  //生成新的查询,
  for each q_new in qset_new// 并行执行
    /* 从邻居列表中查找 q_new要被转发到的远程邻居节点的信息服务地址 */
    {isAddr = lookupNeighbors(q_new.routeTo)
    /* 节点 N_x 生成随机数,作为消息认证的基础,然后向被转发的节点 isAddr 转发该查询,在通信过程中,基于随机数和哈希函数实现消息的认证.在发送消息中,NodeID_is表示节点 isAddr 的标识 */
    R_Nx = genrandom();
    SendMessage(isAddr, N_x, q_new, R_Nx, H(NodeID_is | N_x | q_new | R_Nx));
    /* 节点 isAddr 在接收到消息后,通过自身计算 H(NodeID_is | N_x | q_new | R_Nx)并和接收到的哈希计算结果比较,验证消息是否被篡改.如果被篡改,该条消息被抛弃,否则 isAddr 递归执行查询处理和转发过程. */
    if not verify_m_isAddr(q_new)
        break;
    processAndRoute(q_new, isAddr, client)
  }//end foreach
  //节点返回查询结果,其中需要进行消息认证
  R_Nx = genrandom();
  SendMessage (client, N_x, result, R_Nx, H(client | N_x | result | R_Nx));
  /* 发起查询的客户端所在 DS 引擎节点在接收到消息后,通过自身计算 H(client | N_x | result | R_Nx)并和接收到的哈希计算结果比较,以验证消息是否被篡改,如果被篡改,查询结果被抛弃,否则 client 执行查询结果归并算法. */
  if not verify_m_client(result)
    discard(result);
  combineResult().
```

该算法在一次发现服务查询过程中,将在各相关节点并发执行.在算法执行过程中,通过每个节点部署的访问仲裁模块确定本地查询是否允许以及是否允许进行查询转发,从而实现对供应链信息的保护.在节点之间进行通信时,通过生成的随机数以及哈希函数来进行消息的认证和节点的认证(节点只认证一次,用来建立节点间的信赖关系),从而保证通信过程的安全性.

6 实验

对于分布式发现服务而言,因为其查询算法采用的是递归查询的方式实现对供应链中 RFID 编码的查询,安全机制的应用将会降低系统的响应时间,从而降

低系统的可用性.本节将通过实验验证上述分布式发现服务的安全通信机制在实现安全需求的基础上,在可用性方面,其效率对用户而言也是可以接受的.

为了检验上述分布式发现服务安全通信机制对可用性的影响,在分布式发现服务原型系统 PKU RFID^{3}S 的基础上,实现本文提出的安全通信机制,并对 PKU RFID^{3}S 在增加安全机制前后的相关指标进行对比.

实验的测试数据是人工生成的,在特定的供应链布局下,给出一定数量的不同物品以及产生这些物品的起始节点集合,然后采用以下数据生成规则:一个物品产生后,有四种可能发生的动作(运送到邻居节点、同另一物品组装起来或从一个物品中分离出来、被加工制成新的物品、不再被移动),动作的选择是随机进行的,并且选择"运送到邻居节点"的概率随着该物品路径长度的增加而减小.为了检验未加和已加安全通信机制的两个系统在查询响应时间上的效果,生成的测试数据包含一个最大长度为 20 的供应链、0.5 ~ 1 万个物品和 2.5 ~ 5 万条信息服务事件.

实验主要考察以下指标:

(1)查询命中率:用于验证采用安全通信机制的分布式发现服务的正确性.我们设定查询的超时时间为 20s.查询命中率 = 被发起后在超时时间内返回且结果正确的查询数目/所有查询.

(2)查询平均响应时间:用于评价加入安全通信机制后的分布式发现服务的服务性能.这也是分布式发现服务的主要性能指标.

6.1　实验一

实验一对比在加入安全通信机制前后分布式发现服务对 100 个查询的平均响应时间,每个查询都是从供应链的一个前端开始寻找 10 个不同物品的所有 ObservationEvent 和 QuantityEvent[3],其中 ObservationEvent 描述了"物品仅被观察到但没被处理"这样一类事件;QuantityEvent 描述的事件只关注同一种类物品的数量,而不关注具体的单品.实验结果与预期的结果一致,两个系统返回的结果和预先设置的应该返回的结果相同,说明在加入安全机制前后,分布式发现服务均能返回正确结果,查询命中率在实验测试数据规模下能够达到 100%.

在查询平均响应时间方面,由于随着查询路径的长度的增加,通信时间的增加幅度也随之增加.实验结果表明,随着查询路径长度的增加,加入安全通信机制对平均响应时间的影响是逐渐增大的.这个结果也符合对安全通信机制的分析,因为随着查询路径长度的增加,执行的节点之间的通信次数也随之增加,从而相应的安全机制的执行时间也随之增加.但是从结果上看,未加入安全通信机制的 PKU RFID^{3}S 平均执行时间最长为 3s,而加入安全通信机制后平均执行时间最长为 5s.虽然增加幅度高达 66%,但是最后的结果对于用户来说,属于可接受的范围之内.实验一结果详见图 3.

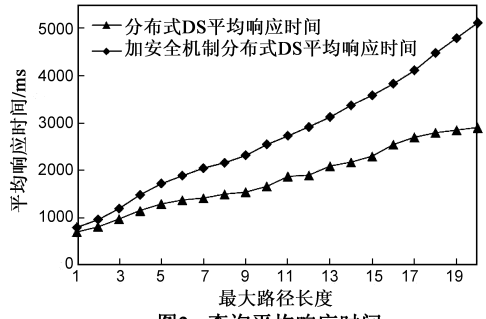

图3　查询平均响应时间

6.2　实验二

实验二对比和实验一相同实验配置下,在加入安全机制前后分布式发现服务对 100 个 BOM 查询的平均响应时间.在这个实验中,物品之间具有 2 ~ 3 层的包含关系,并且每个查询都是寻找与物品相关的所有 ObservationEvent, QuantityEvent, AggregationEvent 和 TransformEvent[3],其中,AggregationEvent 表达了物品的包装/组装与解包装/拆卸的发生;TransformEvent 刻画了多个物品经过加工处理后生成新物品的事件.因此响应时间总体上大于 Recall 查询.

实验结果与预期的结果一致,两个系统返回的结果和预先设置的应该返回的结果相同,说明在加入安全机制前后,对 BOM 查询均能返回正确结果,查询命中率在实验测试数据规模下能够达到 100%.

在查询平均响应时间方面,类似于实验一,随着查询路径的长度的增加,通信时间的增加幅度也随之增加,并且随着查询路径长度的增加,加入安全通信机制对平均响应时间的影响是逐渐增大的.

从实验数据上看,未加入安全通信机制的 PKU RFID^{3}S 执行 BOM 查询的平均执行时间最长为 4s,而加入安全通信机制后平均执行时间最长为 6s.增加幅度为 50%,比例相对于实验一来说有所下降,但增加的绝对量接近.结果表明,加入安全机制对分布式发现服务平均响应时间的影响主要源于查询路径的长度,而与查询类别关系不大.最终结果对于用户来说,属于可接受的范围之内,加入安全通信机制的分布式发现服务保持着较好的可用性.实验二结果详见图 4.

通过实验分析,应用安全通信机制后的分布式发现服务能够正确地提供各类 RFID 编码查询服务,虽然平均响应时间相对于没有应用安全通信机制的分布式发现服务有较大增加,但是仍然在用户可接受的范围之内,具有较好的可用性.

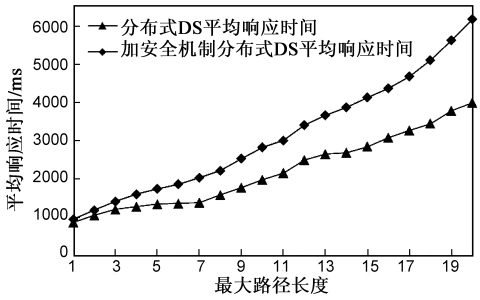

图4 BOM查询的平均响应时间

7 总结

为了满足发现服务查询过程中的安全需求,本文提出了一种基于双随机数的分布式发现服务安全通信机制.在基于 PKI 对分布式发现服务节点进行认证的基础上,在查询过程中,对 RFID 编码进行哈希以保证其私密性,基于双随机数和哈希算法实现消息的认证.

带有安全通信机制的 PKU RFID^{3}S 系统目前已应用于酒类供应链跟踪与防伪,跟踪产品在生产商、批发商、零售商等供应链环节的移动细节,追溯产品来源以达到防伪目的,同时应用安全通信机制,保护生产商、批发商供应链的构成、产品流量和流向等商业秘密信息,确保这些商业秘密不被泄露.实践证明系统在实现安全需求的基础上,时间开销较低,具有较好的可用性.下一步需要进一步挖掘新的安全需求并改进系统性能.

参考文献

[1] VeriSign. The EPC network: Enhancing the supply chain[R]. VeriSign Inc, Mountain View, CA, 2004.

[2] R Agrawal, A Cheung, K Kailing, S Schonauer. Towards traceability across sovereign, distributed RFID databases [A]. Desai B C Proc Of the 10th Intl Database Engineering & Applications Symposium[C]. Delhi, India, 2006. 174 – 184.

[3] EPCglobal. EPC information services (EPCIS) version 1.0.1 specification [S/OL]. http://www.epcglobalinc.org/standards/epcis/epcis_1_0_1-standard-20070921.pdf, 2007-09.

[4] 赵文,李信鹏,等.供应链环境下一种分布式 RFID 发现服务[J].电子学报,2010,38(2A):99 – 106.
ZHAO Wen, LI Xin-peng, et al. A distributed RFID discovery service for supply chain[J]. Acta Electronica Sinica, 2010, 38(2A): 99 – 106. (in Chinese)

[5] Jakkhupan Worapot, Yuefeng Li, Arch-Int Somjit. Design and implement of the EPC discovery services with confidentiality for multiple data owners[A]. Proceedings of the IEEE International Conference on RFID-Technology and Applications[C]. Guangzhou, China, 2010. 19 – 25.

[6] Qiang Yan, Robert H Deng, Zheng Yan, Yingjiu Li, Tieyan Li. Pseudonym-based RFID discovery service to mitigate unauthorized tracking in supply chain management[A]. 2010 Second International Symposium on Data, Privacy, and E-Commerce [C]. Singapore, 2010. 21 – 26.

[7] Trevor Burbridge, Mark Harrison. Security considerations in the design and peering of RFID discovery services[A]. 2009 IEEE International Conference on RFID[C]. Orlando, USA, 2009. 249 – 256.

[8] Liu Xueyang, Zhao Wen, Huang Kaimu, Feng Zhiming, Zhang Shikun, Wang Lifu. A secure communication mechanism of P2P RFID code resolution network[J]. Chinese Journal of Electronics, 2010, 19(4): 621 – 626.

作者简介

赵 文 男,1967 年出生,博士、副研究员,主要研究领域为软件工程、工作流技术和 RFID 相关技术.
E-mail: zhaowen@pku.edu.cn

刘学洋 男,1978 年出生,博士、副教授,主要研究领域为软件工程、信息安全和 RFID 相关技术.
E-mail: liuxueyang@pku.edu.cn