一种智能攻击模型在 RFID 防伪协议中的研究

李 辉,侯义斌,黄樟钦,刘宏珍,何 坚,陈 锐
(北京工业大学嵌入式软件与系统研究所,北京 100124)

摘 要: 本文研究一种 RFID 防伪技术和系统,首先给出了一种基于 RFID 技术的防伪系统软硬件系统架构,进而分析了该防伪系统的层次结构,然后针对系统中防伪安全协议的复杂性提出了智能伪造攻击模型,利用 A * 搜索算法进行路径搜索得到最小攻击代价树,作为对本文提出的防伪系统,尤其是系统中采用的防伪协议的评价. 最后在 VC++ 和 Matlab 环境下对本文提出的模型进行了实验验证,实验结果表明攻击模型对 RFID 防伪协议的验证以及分析是有效的,从而为 RFID 技术与防伪技术的结合提供了一个全新的参考.

关键词: 模型; 协议; 射频识别; 代价树
中图分类号: TP39 **文献标识码**: A **文章编号**: 0372-2112 (2009) 11-2565-09

Research on the Attack Model for RFID Anti-Counterfeit Protocol

LI Hui, HOU Yi-bin, HUANG Zhang-qin, LIU Hong-zhen, HE Jian, CHEN Rui
(*Embedded Software and Systems Institute, Beijing University of Technology, Beijing* 100124, *China*)

Abstract: A RFID technology and anti-counterfeiting system was studied in this paper. Firstly, we propose a hardware and software framework of anti-counterfeit system based on RFID technologies; furthermore the hierarchical structure of the anti-counterfeit system was analyzed in details. Then aimed at the complexity of the anti-counterfeit system an intelligent attacking model was presented here, and the A * algorithm is adopted in this attack model and used to search a lowest price tree by the fictional attacker in order to evaluate the proposed anti-counterfeit system especially for the protocol used in this system. Finally, an experimental testing with VC++ and Matlab was simulated. Simulation results indicate that the proposed modeling methods can be used effectively to model complex anti-counterfeiting systems.

Key words: model; protocol; radio frequency identification (RFID); cost-tree

1 引言

RFID(Radio Frequency Identification)技术是上世纪 80 年代发展起来并日渐成熟的一项通过无线数据采集方式来自动识别物品的技术,近年来发展迅猛. 传统的防伪技术一般不具备唯一性和独占性且容易复制,因此起不到真正的防伪作用. 目前,国际上兴起了电子技术的防伪潮流,尤其是射频标签引起了防伪界的广泛关注. 较早的将 RFID 技术应用于防伪领域的国家主要有美国、欧洲及日本等发达国家,其主要目的是为了实现高效管理. 然而到目前为止,这些 RFID 防伪系统大多只是利用电子标签的唯一 ID 号来实现简单的防伪功能[1,2],目前国际上还没有提出一套基于 RFID 技术的防伪体系架构以及防伪协议. 因此,RFID 防伪技术的研究具有重要的现实和理论意义,是一个值得探索和研究的领域.

本文提出的 RFID 防伪技术结合硬件与软件密码安全技术来实现防伪目标. 主要研究内容是利用各种成熟的密码方案和机制来设计和实现符合 RFID 安全需求的密码协议. RFID 防伪系统的安全可靠性不仅仅取决于系统中安全性最高的个体,而且取决于系统中安全性最为脆弱的环节和实体. 防伪协议是连接防伪系统内部和外部的纽带和桥梁,为了更好的设计协议的结构并且验证协议的有效性,本文通过假想伪造者对整个防伪系统进行攻击,问题转化为攻击者在整个防伪系统空间中寻找目标的求解问题,假设攻击者具有最高水准的攻击技能,以此建立最小代价伪造攻击树,作为防伪系统架构协议层的分析基础,最后采用面向对象的编程技术对伪造攻击模型进行了仿真实验. 仿真试验结果表明攻击者模型对分析复杂的防伪系统是有效的.

2 基于 RFID 技术的防伪系统架构

2.1 防伪架构

本文提出的防伪技术具有如下特点:

(1) 将数字签名技术应用于 RFID 标签生产过程中.

收稿日期:2008-06-16;修回日期:2009-03-01
基金项目:北京市自然科学基金(No. 4072008);国家自然科学基金面上项目(No. 60773186);北京市教委面上项目(No. KM200710005018);教育部科学技术研究重点项目(No. 208003)

赋予每件产品一个唯一标识,此标识在生产、经销、验证等过程中唯一表示此件产品,终身不变.同时将标识生成为一个数字签名写入到 RFID 标签的存储区,然后把标签封装到商品中.

(2)将公、私钥加密认证技术应用于经厂方授权的合法阅读器中并对产品的真伪进行检验.

(3)将 RFID 防伪技术渗透到产品周期中的生产、经销、验证、消费等各环节之中.

(4)将生产者作为防伪系统的中心,掌握防伪系统的各个关键环节.

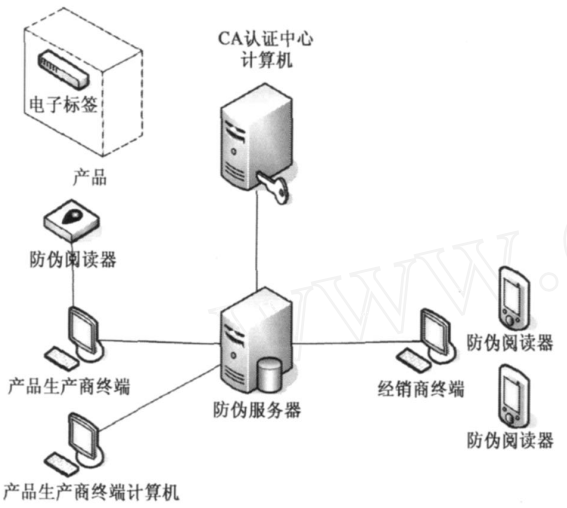

图1 RFID技术防伪系统架构示意图

本文的防伪系统架构由图 1 所示的硬件组成,具体角色如下:

嵌入式防伪阅读器:RFID 防伪系统中的重要设备之一,此设备须由经销商从厂家购进,并通过终端计算机从位于生产厂家的防伪服务器下载防伪数据对产品进行验证.

RFID 防伪电子标签:即 RFID 射频电子标签码,由生产商设定标签并封装到产品中.

防伪服务器:防伪服务器提供阅读器注册、认证,防伪数据下载和产品在线验证等功能.

CA 认证中心:防伪系统的 CA 认证中心,负责各种终端的身份认证.

生产商终端计算机:运行与生产商相关的防伪系统软件,包括:密钥生成与管理子系统、生产子系统和销售子系统.

经销商终端:运行防伪阅读器的辅助程序,完成对产品的在线验证和对防伪阅读器的注册和防伪数据下载.

2.2 防伪系统层次结构

把 RFID 防伪标签和防伪阅读器引入到防伪应用系统中是充分利用了防伪标签以及防伪阅读器本身的安全特性,比如隔离计算和私密存储等.但同时 RFID 技术的引入也使得防伪系统的结构变得更为复杂.RFID 防伪系统的漏洞不仅包括防伪标签和防伪阅读器以及许多中间实体通讯信息交换过程面临的攻击和破坏,而且还包括产品生产商、标签以及阅读器生产商运营过程可能面临的攻击和破坏.因此防伪系统是一个开环的复杂系统,既有内部安全可靠计算通讯平台同时还有包括外部的通讯交互以及商业运营的动态数据更新,它的能力和特性主要体现在系统的防护层次,既包括防伪阅读器和防伪标签的端到端的隔离计算安全,还包括实施身份鉴别、访问授权和接入控制的算法以及密钥管理,同时提供客户的信誉等级评估服务.防伪的质量服务包括认证与授权资源的私密与完整、以及抵抗应用层攻击的能力.面对伪造攻击者手段的层次化特点,本文将防伪系统抽象为一个层次的模型结构.这个层次模型包括 5 个重要层次,由下向上依次如图 2 所示.

图 2 中各个模块的内容和功能描述如下:

(1)防伪物理层:主要包括防伪标签、防伪阅读器、密钥卡、密钥存储服务器.主要功能是支撑防伪系统中的实体,存储有价值或敏感信息的存储;提供隔离的计算环境,避免第三方嗅探;

(2)防伪逻辑驱动层:主要由主控密钥算法,防伪芯片逻辑算法、RFID 编码中间件组成.主要功能是驱动防伪系统的物理实体的逻辑资源;

(3)防伪应用管理层:包括库存管理模块、认证管

图2 防伪层次模块图

理模块、密钥管理模块等防伪系统上层管理的功能实体,主要功能是提供认证服务,防伪数据服务;

(4) 防伪协议层:为防伪系统中各个功能实体之间的通讯提供协议资源服务,如安全信道服务,采用密码措施保证信息的机密性,保证中间状态信息的完整性;

(5) 防伪上层服务策略层,封装各个节点以及资源的信任级别,以及信任情况比较并选择可以采用的安全策略,实施合适的安全措施防护应用系统.

3　防伪协议及智能攻击模型

3.1　防伪协议分析

防伪系统协议首先应该保证防伪标签信息的私密性、完整性和认证性,然后还能挫败攻击者的恶意攻击和破坏,搭建安全可靠的防伪信息传输通道. 因此防伪协议的设计应满足如下目标:

(1) 防止对标签的攻击. 任何非法阅读器不能获取标签的防伪信息.

(2) 防止对标签和阅读器之间通信的侦听.

(3) 防止对用户隐私威胁. 在协议中保证任何与标签有关的编码、识别符等都不能以明文的方式传输.

(4) 防止定位威胁. 确保标签的密钥在每一次与阅读器通讯后都会保持新鲜,这样保证不受定位和跟踪的威胁.

可以用一个五元组来表示 RFID 协议层的目标 $\Omega\{Se, Au, R, Co, Tr\}$,其中 Se 表示私密性,Au 表示可认证性,Co 表示完整性,Tr 表示方跟踪特性,R 表示防克隆.

3.2　RFID 协议的相关研究

国内外提出了很多关于 RFID 数据安全方面的研究方法,但防伪协议研究相对较少. 目前,RFID 安全协议主要有 Hash-Lock 协议、随机化 Hash-Lock 协议、Hash 链协议等[3~7],这些协议各有千秋,下面对此进行简单介绍和分析.

(1) Hash-Lock 协议

Hash-Lock 协议由 Sarma 等人提出. 为了避免信息泄漏和被追踪,Hash-Lock 协议使用 metaID 来代替真实的标签 ID. 协议中没有 ID 动态刷新机制,MetaID 也保持不变,且 ID 是以明文的形式通过不安全的信道传送,因此 Hask-Lock 协议非常容易受到假冒攻击和重传攻击,攻击者也可以很容易地对 Tag 进行追踪[5].

(2) 随机化 Hash-Lock 协议

随机化 Hash-Lock 协议由 Weis 等人提出,协议采用基于随机数的询问-应答机制. 该协议中,认证通过后的 Tag 标识 IDk 仍以明文的形式通过不安全信道传送,因此攻击者可以对 Tag 进行有效的追踪. 同时,一旦获得了 Tag 的标识 IDk,攻击者就可以对 Tag 进行假冒. 该协议无法抵抗重传攻击. 不仅如此,每一次 Tag 认证时,后端数据库都需要将所有 Tag 的标识发送给阅读器,二者之间的数据通信量很大. 所以,协议就可能存在安全性和实用性缺陷[6].

(3) Hash 链协议

本质上 Hash 链协议也是基于共享秘密的询问-应答协议[7]. 阅读器发起认证,Tag 总是发送不同的应答. 在该协议中,Tag 成了一个具有自主 ID 更新能力的主动式 Tag. 同时,Hash 链协议是一个单向认证协议,只能对 Tag 身份进行认证,不能对阅读器身份进行认证. 因此 Hash 链协议非常容易受到重传和假冒攻击.

3.3　RFID 防伪安全协议

防伪协议的设计目标主要体现在每个防伪标签使用不同的密钥来保护,每个标签的密钥都是在标签生产过程中采用 SHA-1 加密算法把共享私钥信息与标签的唯一序列号进行数字签名得到的. 每次会话都由存储在标签内的私钥与伪随机数产生一个新的会话密钥,防止物品被跟踪. 防伪协议的认证是指防伪标签以及防伪中心对防伪阅读设备的合法性进行的验证. 认证的原理是合法的阅读设备和防伪标签应该共有相同的认证密钥,伪造的读写设备或标签无法获得相应密钥. RFID 防伪协议交互图如图 3 所示. 以下是防伪标签对防伪阅读器的认证过程.

阅读器把明文信息以及通过 RC4 构造的验证信息 MRC4 经会话加密后传送给标签,密钥变更协议报文通过名文传送给标签. 验证的流程如图 4 所示,验证信息加密过程具体如下:

(1) 首先由密钥协商完成算法完成会话密钥的协商,形式化描述如下:

$$PK = NotiP(sharekey, head)\ (head \in NotifyM) \quad (1)$$

验证信息用 RC4 算法产生,认证报文信息构成如下:

$$Ci = RC4(message, privatekey),\ mi \in R \quad (12)$$

(2) 验证信息必须以密文进行传送,验证信息传送中不能出现明文.

$$m_i = crypt(message, Ci, privatekey),\ mi \in R \quad (3)$$

(3) 阅读器发送给认证标签协商会话的报文构成,形式化为:

$$N_i = NotifyM(message),\ Ni \in R \quad (4)$$

(4) 阅读器发送给标签的认证信息采用会话密钥进行加密形式化表示如下:

$$Sendmessage = Ni\ \&\&Mi; \quad (5)$$

标签对阅读器的验证过程始于接收到阅读器的认证信息,认证解密流程如图 5 所示,从图 5 中可以看出收到信息中包含会话密钥更新报文及经过加密以后的验证信息. 标签首先从信息中提取出密文以及会话密

钥随机数,然后通过共享密钥进行更新获取当前的会话密钥. 用会话密钥对接收到的密文解密,解密出原文,对原文进行完整性检验,比较得到的验证报文 MIV' 与接受到的 MIV,相同则阅读器经过认证,不同则阅读器没有经过认证. 协商过程结束.

解密过程具体描述如下:

(1) 根据阅读器传送过来的信息解析获得密钥变更协议(明文形式)和验证信息(密文形式)

$$Mi = NotiP + cryptmi \quad , \quad Mi \in T \tag{6}$$

(2) 根据解析出来的密钥变更报文内容和合法阅读器自带的共享密钥采用 SHA_1 算法生成私钥.

$$PK = NotiP(sharekey, head) \quad , \quad head \in NotifyM \tag{7}$$

(3) 利用私钥对接受到的密文解密,解密出内容信息包括验证信息和验证信息的校验文:

$$DMi = dcrypt(cmi, MCR4) \quad , \quad Mi \in T \tag{8}$$

(4) 对解密出来的验证信息采用 R4 算法生成验证报文:

$$CR4(DMi, MCR4') \tag{9}$$

(5) RFID 标签根据 MCR4' 与 MCR4 进行比较,如果不同,发送销毁命令,并进入死锁状态. 否则进入应答状态.

If (MCR4' == MCR4) then goto KillTag;

Else goto reply;

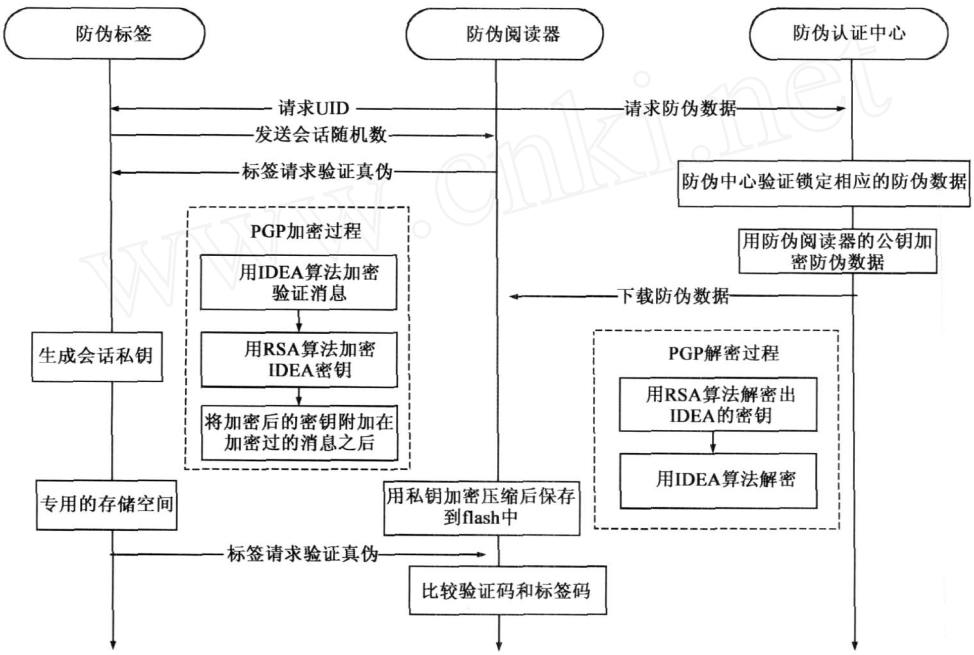

图3 认证协议交互图

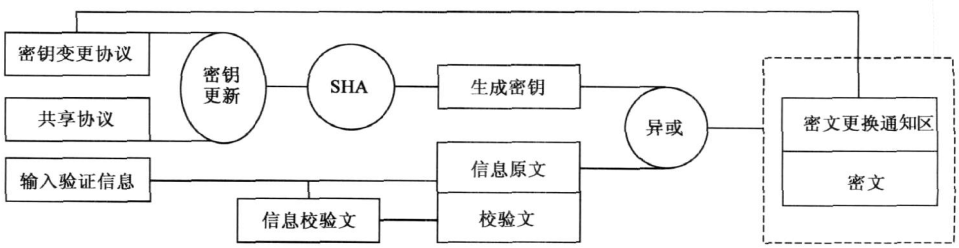

图4 验证信息加密过程图

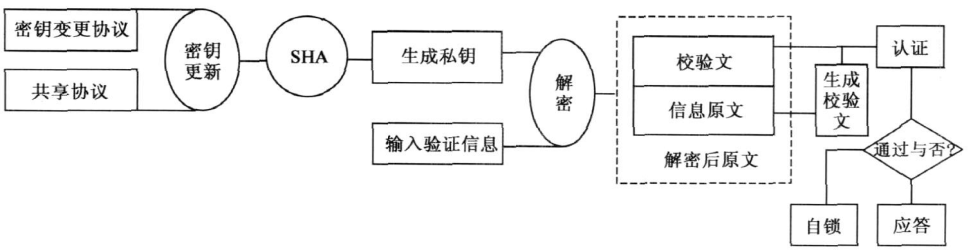

图5 验证信息解密过程图

3.4　智能攻击模型

从防范原理上说不可能设计出能够抵抗一切攻击和破坏的完善系统,RFID 防伪系统也不例外. 虽然采取各种不同的软件和硬件安全防护措施,必须认识到所有当前可用的防范对策无法抵抗未来可能出现的一切攻击;我们的设计原则是采用芯片制造技术、和软件密码技术的有效组合使得攻击者成功实施破坏的成本急剧增加,从而撼动攻击者的利益.

本文在 RFID 层次模型的基础上提出了伪造者攻击模型,假设伪造者对整个防伪系统进行攻击,因此可以把问题描述为攻击者在整个防伪系统空间中寻求造假途径的问题,假设攻击者具有最高水准的攻击技能. 表 1 列出了部署防伪系统中的节点以及各个节点之间的相互关系,正如本文前面对节点的定义所指出的节点是对防伪措施的一种抽象,"节点"并不代表防伪系统中的实际节点,比如 n 个标签也只是防伪系统中的一种防伪措施,n 个标签只代表一个节点. 表中 Na 表示节点之间没有任何关联.

表 1　防伪措施和节点对应关系表

	标签 V1	阅读器 V2	数据中心 V3	加密算法 V4	会话密钥 V5	主控密钥 V6	电路实体 V7
标签 V1	Na	空中接口	Na	认证协议	会话协议	Na	密码算法
阅读器 V2	空中接口	Na	安全信道	电路逻辑	密钥协商	Na	密钥算法
数据中心 V3	阅读器	身份认证	Na	PKI	数字签名	密钥更新	Na
加密算法 V4	电路逻辑	电路逻辑	存储磁盘	多重加密	一次一密	密钥生成	存储芯片
会话密钥 V5	安全信道	安全信道	密钥存储	一次一密	会话序列	加密算法	Na
主控密钥 V6	Na	密钥生成	Na	密钥生成	密钥生成	Na	Na
电路实体 V7	VHDL	VHDL	Na	电路逻辑	Na	Na	Na

我们将表 1 中各节点 V1-V7 的连通关系用网络图表示为图 6. 图中深色节点表示防伪系统中部属的各防伪节点,边表示两个节点之间存在物理或者逻辑关联,比如节点标签 V1 和阅读器 V2 节点之间通过空中接口关联,图中虚线半圆表示节点自己和自己有关联关系.

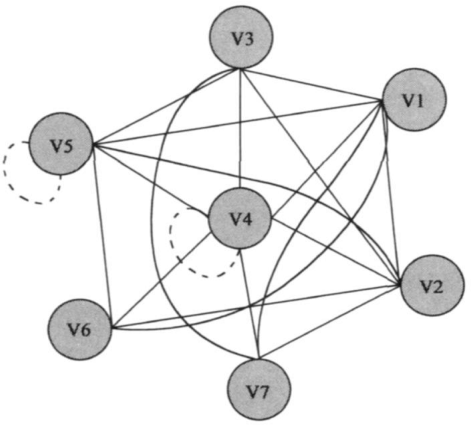

图6　节点关联网络图

3.5　伪造攻击模型知识描述

防伪问题知识表述:设有一个由 RFID 技术为核心的防伪系统,其中包括密码算法、密钥管理协议、VHDL 实现以及防伪协议等物理和逻辑资源,有一个攻击者试图采用各种手段最终达到能够伪造商品并且通过防伪系统检验的目的.

定义 1　防伪系统问题描述:设有一个由 RFID 技术为核心构成的防伪系统记做 S.

定义 2　防伪措施节点:密码算法、密钥管理协议、RFID 标签以及 RFID 防伪协议等物理和逻辑的资源组成防伪空间节点记做 a.

定义 3　攻击者:有一个攻击者(Attacker)试图采用各种手段最终达到能够伪造商品目的的途径记做 P.

根据上述的定义我们就可以把防伪系统 S 逆向转化为伪造攻击者在防伪系统中进行逆向攻击,寻找最佳路径 P 的过程,Search 是伪造攻击者在防伪系统 S 寻找最佳路径所采用的智能搜索算法,公式表示为:

$$S \Leftrightarrow \text{Search}(\text{Attacker}, a, P)$$

定义 4　造假攻击路径代价是指由于系统分布在防伪终端或中间环节的功能节点受到造假者攻击时,防伪系统中相应的措施或手段给造假者带来的代价. 符号表示 $f(a) = lv(a) + pv(a)$,其中 $lv(a)$ 表示造假者进行逻辑攻击造假所付出的代价,$pv(a)$ 表示造假者物理攻击所付出的代价.

定义 5　初始节点是指伪造攻击者开始攻击的节点,表示 S_0.

定义 6　局部代价表示造假攻击者从一个防伪空间中的一个环节攻击到另一个环节所付出的代价,表示为 $H(a, \beta)$.

定义 7　目标节点状态表示伪造者在防伪空间最终造假成功的节点,符号为 E.

定义 8　防伪系统状态空间表示防伪系统中所有的物理节点以及防伪协议构成的空间,符号为 Ω.

定义 9　状态空间节点代价表示防伪系统中所有成员给攻击者带来的代价,符号为 $N(\Omega_0)$.

定义 10　造假攻击树表示为 $T(p, v)$,其中 v 表示造假者达到目标节点所需的最小代价路径,p 表示造假者所采用的路径.

3.6 防伪逆向空间搜索算法

在防伪系统层次化建模基础上,把防伪系统描述为一个图的数据结构,在对图的搜索算法中启发式 A* 算法由于具有向下搜索的前瞻性,而且具有较高的搜索效率,因此本文采用启发式 A* 算法搜索来模拟造假者寻找造假途径的过程,也就是 3.5 节中的 Search. A* 算法主要通过估价函数 $f(n)$ 来选择后续有价值的节点. 这种方法能够减少搜索范围,减少搜索量,优于宽度优先搜索和深度优先搜索方法. 估价函数的设计是启发式搜索的关键[8~11](3.7 节详细介绍估价函数).

伪造攻击模型知识抽象表述中各个节点 α 是指采用的伪造攻击操作所花费的时间和物质代价. 设计两个 OPEN 和 CLOSE 单链表,它们都不包含重复节点. 其中 OPEN 表存放已生成但还未扩展的防伪节点. CLOSE 表存放已经完成扩展的节点,即伪造攻击节点.

整个算法可以描述为:

(1) 把初始节点 S_0 排在首位放入 OPEN 的未扩展节点表中,并建立一个叫做 CLOSE 的已扩展节点表,其初始为空;

(2) 若 OPEN 表为空,则搜索失败,退出;

(3) 移出 OPEN 表中的第一个伪造代价节点放入 CLOSE 表中,记该结点为 N;

(4) 若 N = 目标结点,则搜索成功,结束;

(5) 若 N 不可扩展,转(2);

(6) 扩展 N,生成一组子结点,将这些子结点放到 OPEN 表中;

(7) 按估价函数 $f(n)$ 对 OPEN 表中的结点从小到大排序,转(2).

规则:防伪系统中的所有攻击手段的代价是动态变化的,如类似的攻击手段一旦被造假者掌握,类似节点的攻击代价是动态变化的. 规则符号表示为:

```
For each Point In Path ∈VS
    IF GAIN(POINT1) = TRUE
        THEN
        V1 (point) = 1/2 V(point)
    End if
```

3.7 估价函数设计

A* 算法[12]引入了估价函数 $f(n)$,它是对价值函数 $f^*(n)$ 的估计,价值函数 $f^*(n)$ 表示从初始结点 s 经过结点 n 到达目标结点最小可能花费的代价. $f^*(n)$ 包括两部分:一是从初始结点 s 到结点 n 的最小代价,记为 $g^*(n)$;另一部分是从结点 n 到目标结点的最小代价,记为 $h^*(n)$,价值函数 $f^*(n) = g^*(n) + h^*(n)$. $f(n)$ 是对函数 $f^*(n)$ 估计,也可以分为 $g(n)$ 和 $h(n)$ 两部分;$g(n)$ 是对 $g^*(n)$ 的估计,对 $g(n)$ 来说,$g(n) = 0$,$n = s$ 为初始节点;$g(n) = g(m) + Q(m, n)$,n 为 m 的子结点,边 (m, n) 的权值为 $Q(m, n)$. $h(n)$ 是对 $h^*(n)$ 的估计,它一般根据经验所得,而且各个具体问题各不相同,无规律可寻. 之所以引入 $h(n)$ 是因为在搜索前无法得知 $h^*(n)$,而用 $h(n)$ 是对 $h^*(n)$ 估计,A* 算法找到目标结点后得到路径可能不是最优的路径,而是由经验所得的近似最优路径[13~15].

本文的模型所描述的伪造代价是指攻击者针对防伪系统进行攻击所付出的代价,伪造代价作为估价函数的评估依据主要遵循以下规则:

规则 1:攻击防伪系统不同的层次见防伪层次模块图 2,难度也不相同,层次越高难度越大.

规则 2:根据攻击者的攻击手段不同,可以把攻击手段分为物理攻击和逻辑攻击两种. 物理攻击主要包括对加密芯片以及防伪标签等物理节点的分析与破译. 逻辑攻击主要包括对密码、加密算法、认证协议的分析与破坏. 攻击者对物理硬件攻击所需要的专用设备以及分析仪器价格都比较高昂,因此物理攻击付出的代价高于逻辑攻击的代价.

规则 3:攻击无线网络协议的代价小于有线网络协议的代价.

规则 4:破获密码的代价要大于破解算法. 攻击独立非网络实体数据的代价要高于网络环境实体的代价. 这里的代价既包括破解防伪节点所付出的时间代价也包括破解所需要设备付出的物质方面的代价.

在估价函数中 $g(n)$ 表示从初始节点到当前节点 n 的实际代价,考虑到希望 $g(n)$ 在估价函数中的权重问题,所以 $h(n)$ 不能取得太大,否则 $g(n)$ 所占比重过小,无法体现经过路径的代价. $h(n)$ 也不能取得过小,过小导致估价函数智能性降低,特别是如果取 $h(n) = 0$,则退化为盲目搜索的广度优先搜索. 综合考虑,取 $h(n) = C1 * ml * lv + C2 * ml * pv$;其中取 ml 代表防伪系统的层次,vl 代表逻辑攻击手段所付出的代价,pv 代表物理攻击所付出的代价,$C1$ 代表逻辑攻击的加权系数,$C2$ 代表物理攻击的加权系数.

3.8 攻击代价分析

攻击者希望以最小的代价攻击目标. 因此最小攻击代价分析就是指对攻击者到达攻击目标所经过的最佳路径进行分析.

定义 11 攻击树是指攻击者到达目标节点所经过的路径. 符号为:*TAttack*.

定义 12 攻击最小代价树,成功伪造攻击所付出的代价表示为:

$$TAttackCost = \sum_{i}^{n} nodecost(i) \tag{10}$$

其中 i 表示攻击过程的节点序号, n 表示攻击过程的子攻击数目, $nodecost(i)$ 表示第 i 个子攻击成功需要付出的代价.

定义 13　部署相应的防伪措施所付出的代价称为防伪代价树. 其中防伪代价树的结构与防伪系统不是一一对应的. 因为有的防伪措施与多个伪造节点相对应,也有的情况是多项防伪措施为了应对某项伪造手段. 符号表示为:

$$TAntiCost = \sum_{i}^{n} nodecost(i) \qquad (11)$$

其中 i 表示攻击过程的步骤序号, n 表示攻击过程的子攻击数目, $nodecost(i)$ 表示第 i 个子攻击成功需要付出的代价.

攻击代价分析采用逆向分析方法,所谓逆向分析就是指站在攻击者的立场进行分析,分析攻击者破译防伪措施节点所付出的代价.

(1) 分析攻击最小代价树的每个节点,从中找到防护链的脆弱点.

(2) 计算新的防伪措施代价树 $TAntiCost$,同时重新计算攻击最小代价树 $TAttackCost$.

4　仿真试验结果

本文采用 VC++6.0 开发实现模型的仿真程序. 实验环境是 VC++ 和 Matlab,参数包括:初始化节点个数、初始化防伪专家知识库,知识库包括破译密码的时间代价,破解芯片所需购置的设备代价,以及获得相应专业知识的代价. 仿真程序中用到的结构体和类如下:

```
typedef struct AttackState
{
    int postitionstate[6][6];//存储每个防伪节点在层次模型中的位置
    struct AttackState *prestate;//上一个结点的指针
    struct AttackState *nextstate;//下一个结点的指针
}TAttackState;//定义防伪系统架构
class CAttackTree
{
public:
TAttackState StateInit;//初始状态
TAttackState StateObj;//目标状态
TAttackState StateCur;//当前状态
CPtrList OpenList;//Open 表
CPtrList CloseList;//Close 表
CPtrList ResultList;//保存结果
TAttackState *curstep;
public:
int mrndepth;//搜索深度
CJiuG();
};
```

通过伪造事件驱动程序,可以加载防伪系统的部件,然后设置好目标节点. 仿真程序流程图如图 7 所示. 仿真程序主要有以下几个模块:

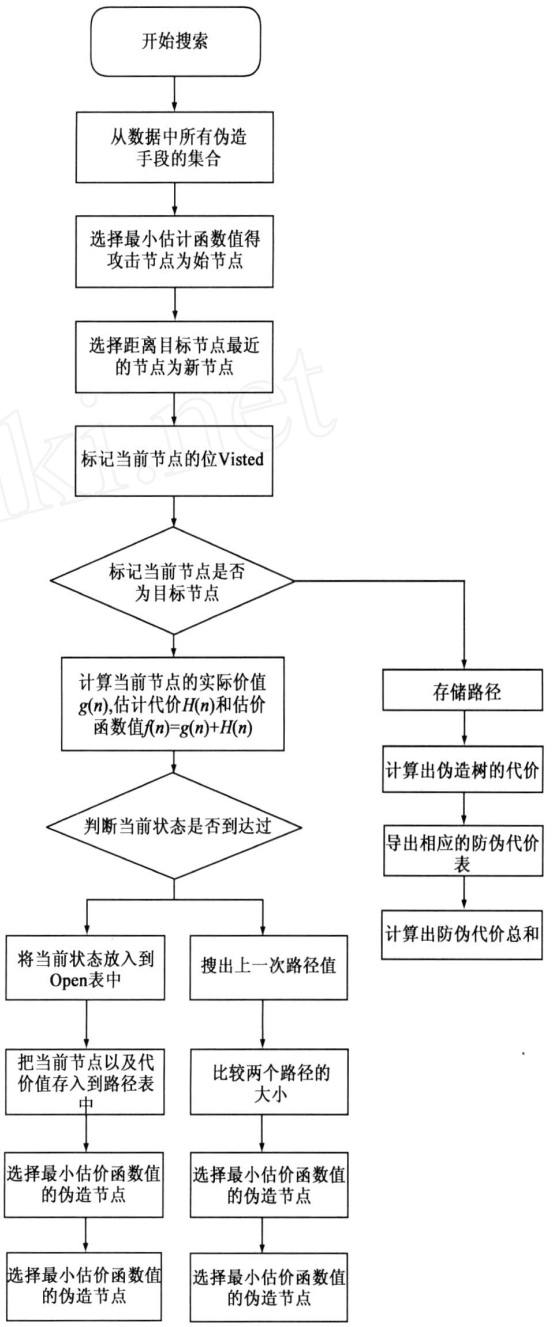

图7　仿真程序模块结构图

(1) 维护模块:主要功能是维护是 OPEN 表以及 CLOSED 表两个队列. 负责队列中节点的排序以及删除添加等功能.

(2) 存储模块:主要功能是存储伪造攻击最小代价路径以及路径中每个节点的代价.

(3) 最小攻击代价树映射模块,主要功能是把攻击链中的每个节点的功能映射于防伪节点上,同时计算

其代价.

(4) 核心算法模块:通过攻击事件驱动防伪模型实体搜索最佳路径的算法模块.

图 8 是仿真实验之后得到的代价最小的达到伪造目的的路径. 如图 8 所示伪造者开始伪造的第一步是购买防伪商品并获得标签,标签是防伪商品厂家采取的第一道防伪措施对应本文中的节点 1,伪造者接下来要对标签编码进行分析,也就是图 7 中的初始化节点,阅读器是真品厂家采取的第二道防伪措施对应文中的节点 2,标签和阅读器之间通过空中接口协议通讯并进行身份认证,同时伪造者要分析标签的芯片结构以及电路. 假设伪造者通过侦听获取到了阅读器和标签之间的空中接口协议,那么他们还得获取主控密钥,也就是本文对应的节点 3,假设他们又成功获得主控密钥,如果他们没有会话密钥依然不能达到伪造目的,因为他们通过主控密钥与加密算法的运算才能获得会话密钥,只有获得了这个密钥才能写入标签,最终伪造成功. 造假者不仅要成功地克隆标签,由于标签中密钥保护,他们还必须获得各种密钥,尤其是主控密钥,而主控密钥保存在防伪系统的核心管理层,造假者必须付出巨大的代价并冒着暴露身份的风险才有可能造假成功,这样给造假者带来了高昂的代价,因此最终迫使利益驱动的造假者放弃造假行为.

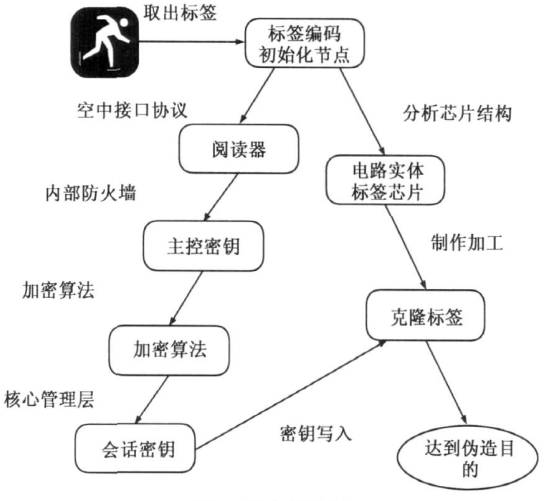

图8 最小代价树

通过以上分析可以得出结论:防伪标签以及防伪阅读器双方的三次认证握手认证协议可以增大攻击者的难度,迫使伪造攻击者不仅要对标签的结构进行分析,同时还要获取写入标签中的会话密钥. 同时为了隔断攻击者通过协议分析攻击到主控密钥的控制中心,防伪阅读器应采用隔离计算,阅读器的防伪计算不依赖后台主机以及网络通讯,因此防伪系统中采用独立的嵌入式防伪阅读器.

仿真实验结果得到了 7 个节点的攻击防伪路径以及最终达到伪造目的的代价,具体结果见图 9. 图中纵坐标表示攻击成本和攻击获利后的代价比,横坐标表示防伪系统中的防伪措施节点数目. 对于防伪系统的部属者,通过设置算法及加密密码本身不增加正常生产成本,比如在防伪系统防火墙中或者阅读器中,增加多道防御措施,由于属于算法的编程与设置,因此并不会增大防伪系统的生产成本. 但是通过设置多重加密算法以及密码的做法,却极大增加了造假者解密复制成本. 因此随着系统节点的增加,伪造成本急剧增长,而防伪成本却趋于平稳增长. 当攻击者所付出的代价低于获利时,造假活动就失去了意义.

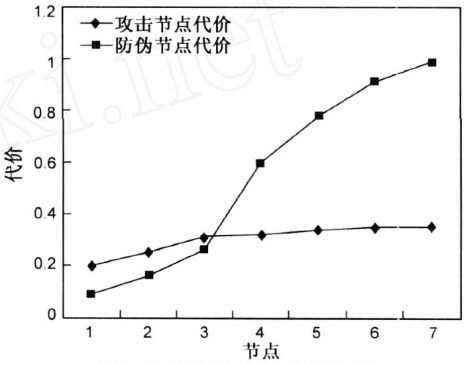

图9 防守和攻击节点代价图

5 结论

本文研究一种 RFID 防伪技术和系统,提出了基于 RFID 技术的防伪系统软硬件架构. 针对防伪系统中防伪协议设计的复杂性提出了智能伪造攻击模型,通过人工智能中的 A* 搜索算法进行路径搜索的最小攻击代价树,计算了伪造者攻击成功的代价,以此为根据量化防伪协议在防伪系统中的作用. 由仿真结果可以看出本文所提出的模型能够形式化分析复杂防伪协议的设计,提高防伪系统的安全可靠性.

参考文献:

[1] R Weinstein. RFID:a technical overview and its application to the enterprise[J]. IT professional,2005,7(3):27 - 33.

[2] J L M Flores,et al. A performance of RFID tags in near and far field[A]. Proceedings of IEEE International Conference on Personal Wireless Communications (ICPWC)[C]. New Delhi, India:IEEE Press,2005,143:353 - 357.

[3] M Ohkubo, K Suzuki, S Kinoshita. Hash-chain based forward-secure privacy protection scheme for low-cost RFID[A]. Proceedings of the 2004 Symposium on Cryptography and Information Security (SCIS 2004)[C]. Berlin: Springer Verlag Press,2004. 719 - 724.

[4] S E Sarma,S A Weis,D W Engels. RFID systems and security

and privacy implications[A]. Proceedings of the 4th International Work-shop on Cryptographic Hardware and Embedded Systems (CHES2002)[C]. Berlin: Springer-Verlag Press, 2003,2:454 - 469.

[5] S E Sarma, S A Weis, D W Engels. Radio-frequency identification:Secure risks and challenges[J]. RSA Laboratories Cryptobytes, 2003, 6(1):2 - 9.

[6] S A Weis, S E Sarma, R L Rivest, D W Engels. Security and privacy aspects of low-cost radio frequency identification systems[A]. Proceedings of the 1st International Conference on Security in Pervasive Computing[C]. Berlin: Springer Verlag, 2004. 201 - 212.

[7] D Henrici, P Muller. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers[A]. Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW '04)[C]. Washington, DC, USA: IEEE Computer Society, 2004. 149 - 153.

[8] 武虎,李少远. 基于局部信息的滚动优化与机器人路径规划[J]. 系统仿真学报, 2004, 17(8):1680 - 1684.
WU Hu, Li Shao-yuan. Receding horizon optimization under local environment for robot path planning[J]. Journal of System Simulation, 2005, 17(8):1680 - 1684. (in Chinese)

[9] L P Swiler, C Phillips, D Ellis, et al. Computer-attack graph generation tool[A]. Proceedings of DARPA Information Survivability Conference & Exposition II[C]. Washington, DC, USA: IEEE Computer Society, 2001. 307 - 321.

[10] R Ritchey, P Ammann. Using model checking to analyze net work vulnerabilities[A]. Proceedings of IEEE Symposium on Security and Privacy[C]. Washington, DC, USA: IEEE Computer Society, 2001. 156 - 165.

[11] O Sheyner, J Haines, S Jha, et al. Automated generation and Analysis of attack graphs[A]. Proceedings of the IEEE Symposium on Security and Privacy[C]. Washington, DC, USA: IEEE Computer Society, 2002, 1:142 - 149.

[12] 王士同. 人工智能教程[M]. 北京:电子工业出版社, 2001.
Wang Shi-tong. Artificial Intelligent Course[M]. Beijing: Electronic Industry Press, 2001. (in Chinese)

[13] Xin Ming Ou. A logic-programming approach to network security analysis: [PhD dissertation][D]. Princeton: Princeton University, 2005.

[14] Pammann, J Pamula. A host based approach to network attack chaining analysis[A]. Proceedings of the 21st Annual Computer Security Applications[C]. Washington, DC, USA: IEEE Computer Society 2005, 2:456 - 467.

[15] 刘道斌,郭莉,白硕. 基于 Petri 网的安全协议形式化分析[J]. 电子学报, 2004, 32(11):7290 - 7294.
Liu Dao-bin, Guo Li, Bai Shuo. Safety protocol formalization analysis based on Petri net[J]. Acta Electronica Sinica, 2004, 32(11):7290 - 7294. (in Chinese)

作者简介:

李　辉　男,1971 年 2 月出生于吉林省吉林市. 1994 毕业于吉林大学获学士学位,2004 年于吉林大学获硕士学位,现为北京工业大学计算机学院博士研究生,主要研究方向:嵌入式软件与系统、计算机应用技术、人机交互系统.
E-mail:hli3302@gmail.com

侯义斌　男,1952 年 4 月出生于陕西. 教授、博士生导师. 1981 年获西安交通大学计算机系工学硕士学位、1986 年获荷兰 EINDHOVEN 科技大学工学博士学位. 现任北京工业大学副校长、软件学院院长. 研究方向为:嵌入式软件与系统、新型人机交互、环绕智能. 发表科技论文百余篇,学术专著一部,发明专利四个,科教电影一部;获国家教委科技进步二等奖两项.