



(12)发明专利

(10)授权公告号 CN 105871904 B

(45)授权公告日 2018.08.24

(21)申请号 201610357372.9

CN 104363096 A, 2015.02.18,

(22)申请日 2016.05.25

CN 104363097 A, 2015.02.18,

(65)同一申请的已公布的文献号

CN 101114901 A, 2008.01.30,

申请公布号 CN 105871904 A

CN 101452539 A, 2009.06.10,

(43)申请公布日 2016.08.17

CN 104219046 A, 2014.12.17,

(73)专利权人 电子科技大学

CN 101535845 A, 2009.09.16,

地址 611731 四川省成都市高新区(西区)
西源大道2006号

CN 102236773 A, 2011.11.09,

(72)发明人 许春香 张源 温俊伟 金春花
何瑜

CN 103699920 A, 2014.04.02,

(74)专利代理机构 成都点睛专利代理事务所
(普通合伙) 51232

CN 104901812 A, 2015.09.09,

代理人 葛启函

US 2012/0268239 A1, 2012.10.25,

(51)Int.Cl.

US 2008/012688 A1, 2008.01.17,

H04L 29/06(2006.01)

Jens Hermans等.Efficient, Secure,

(56)对比文件

Private Distance Bounding without Key

CN 104113414 A, 2014.10.22,

Updates.《WiSec '13: Proceedings of the

(54)发明名称

sixth ACM conference on Security and

一种用于RFID的限定距离的安全认证方法

privacy in wireless and mobile networks》

(57)摘要

.2013,

本发明属于通信技术领域,具体的说涉及一种用于RFID的限定距离的安全认证协议。本发明主要方法包括:标签发起认证请求并发送一个随机数给阅读器,阅读器回应一个随机数给标签;标签与阅读器通过各自的私钥,对方的公钥以及接收到的随机数计算认证值;同时标签与阅读器间进行n轮时序严格的会话,用来验证限定距离;阅读器接收并检验标签计算的认证值是否合法,同时检验标签的距离是否有效,若通过,则认证通过,否则认证失败。本发明的有益效果为,除了能够使得阅读器对标签的身份进行认证,还能对标签与阅读器之间的距离进行认证。

审查员 程梦莉

权利要求书2页 说明书4页

1. 一种用于RFID的限定距离的安全认证方法，包括：

初始化：生成阅读器与标签的公私钥，在阅读器中存储阅读器的私钥与标签的公钥，在标签中存储标签的私钥与阅读器的公钥；通过阅读器确定最大限定距离；

阅读器认证标签：标签发起认证请求并发送一个随机数给阅读器，阅读器回应一个随机数给标签；标签与阅读器通过各自的私钥，对方的公钥以及接收到的随机数计算认证值；同时标签与阅读器间进行n轮时序严格的会话，用来验证限定距离；阅读器接收并检验标签计算的认证值是否合法，同时检验标签的距离是否有效，若通过，则认证通过，否则认证失败；

所述生成阅读器与标签的公私钥的具体方法为：

根据安全参数l，发行者选取对应的椭圆曲线群G与模为p的整环Zp，从Zp中随机选取一个y作为阅读器的私钥，并计算Y=yP作为阅读器的公钥；从Zp中随机选取一个x作为标签的私钥，并计算X=xP作为标签的公钥；将x, Y秘密发送给标签，将y, X秘密发送给阅读器；其中，G的阶为p，生成元为P；

通过阅读器确定最大限定距离的具体方法为：

根据安全参数l，阅读器确定一个合法标签与自己之间的最大距离 \in ；同时根据 \in 与系统参数，阅读器确定进行通讯的最大轮数n和一轮通信所需的最大时间 Δt ；

阅读器认证标签的具体方法为：

a. 标签从Zp中随机选取一个r1，并计算R1=r1P，标签将R1发送给阅读器；阅读器从Zp中随机选取一个r2，并计算R2=r2P，阅读器将R2发送给标签；

b. 标签首先计算L=r1Y+xR2 \in G，因为R1, R2, L \in G，且G是基于椭圆曲线的循环群，所以R1, R2和L是椭圆曲线上的点，因此，标签得到L的横坐标值，用xcoord(L)来表示；标签取xcoord(L)的前2n位，用[xcoord(L)]_{2n}来表示；最后标签将[xcoord(L)]_{2n}的前n位赋值给t⁰，将[xcoord(L)]_{2n}的后n位赋值给t¹；

c. 阅读器计算[xcoord(yR1+r2X)]_{2n}，并将[xcoord(yR1+r2X)]_{2n}的前n位赋值给t⁰，将[xcoord(yR1+r2X)]_{2n}的后n位赋值给t¹；阅读器从Zp中随机选取一个e'，并根据通讯轮数n，首先将e'使用一个哈希函数映射为长度为n的比特串，即e=f(e')；其中f(•):{0,1}*→{0,1}ⁿ是一个映射到n比特的哈希函数；随后阅读器将e分为n比特，其中第i比特用(e)_i(i \in [1,n])来表示，令c_i=(e)_i；

d. 阅读器与标签开始n轮时序严格的会话，具体为：阅读器将c₁至c_n依次发送给标签，并且在发送c₁时开始计时；每次当标签收到c_i(i \in [1,n])后，存储c_i，计算f_i=(1-c_i)(t⁰)_i+c_i(t¹)_i，并将f_i发送给阅读器，其中(t⁰)_i代表t⁰的第i比特，(t¹)_i代表t¹的第i比特；阅读器收到f_i后，计算f_i*=(1-c_i)(t⁰)+c_i(t¹)_i，并验证等式f_i*=f_i是否成立；若对于i \in [1,n]，任意一个i时，等式f_i*=f_i不成立，则认证失败；否则，在验证完成f_n*=f_n后，进行下一轮会话；任意一个i时，会话完成时停止计时，并在第i+1次会话开始时重新计时；设第i轮会话共需时间为τ_i(1≤i≤n)；

e. 阅读器将e发送给标签；标签收到e后，验证c₁||c₂||…||c_n=e是否成立；若成立，标签将t⁰||t¹发送给阅读器；

f. 阅读器首先验证等式t̃⁰||t̃¹=t⁰||t¹是否成立，若不成立，则认证失败；否则，阅读器验证

$\tau_i \leq \Delta t$ ($1 \leq i \leq n$) 是否成立, 若不成立, 则认证失败; 否则, 认证成功。

一种用于RFID的限定距离的安全认证方法

技术领域

[0001] 本发明属于通信技术领域,具体的说涉及一种用于RFID的限定距离的安全认证方法。

背景技术

[0002] 无线射频识别 (Radio Frequency Identification,RFID) 是一种具有非物理性接触、低成本、低功耗等特点的自动识别技术。在RFID系统中,阅读器与标签之间通过无线射频信号来传递信息,从而识别被标识物体的信息。由于RFID技术具有无需人工干预,无需物理接触以及便于操作等传统识别技术所不具有的优点,所以它广泛应用于当前基于云计算与物联网环境的诸多行业。这使得RFID技术在人们的生活中占有重要的地位。

[0003] 然而,随着RFID技术的大规模普及,存在于其中的安全问题受到了人们的广泛关注。由于RFID系统中阅读器与标签之间是通过无线射频信号进行通信的,信号传递的过程中容易遭受到恶意攻击,这使得敌手可以通过对信号的窃听、拦截、篡改与重放等手段,达到窃取标签信息,假冒合法用户与瘫痪RFID系统等目的。为了防止这样的敌手,保证RFID系统的安全性,在标签与阅读器之间引入认证机制是一种行之有效的手段。换句话说,在阅读器与标签开始会话前,阅读器首先要认证标签的身份信息,如果认证通过,阅读器才会与标签进行进一步会话。这样的机制能够有效挫败敌手的伪造与冒充,极大的提高了RFID系统的安全性。

[0004] 为了保证RFID系统中认证机制的有效性和安全性,作为构建认证机制的基础,认证协议的设计与选取就尤为重要。若认证协议本身存在安全问题,那么这种安全问题同样会存在于其构建的认证机制中。现有的很多认证协议能够保证认证的安全性。然而,绝大多数协议并没有考虑认证距离的问题,即需要阅读器进行认证的标签是否在一个合法的物理范围内。这使得它们不能很好的应用于对于很多限定距离的RFID认证系统。具体来说,限定距离RFID主要用于对识别距离有特殊要求的应用场合,设计初衷是为了解决了高频RFID普遍存在的识别距离不稳定、抗攻击能力差以及为了弥补前面两点采取大功率发射器带来的辐射危害等问题。限定距离RFID系统使用范围包括:小范围精确识别(办公室门禁、电梯控制系统)、中型距离识别(企业、小区、学校、办公楼车辆一卡通)、远距离识别(政府和企事业单位办公大楼远距离车辆识别系统、ETC和航空管制)。因此,如何能在限定距离的RFID系统中进行安全的认证是现阶段RFID认证协议的研究重点与难点。

发明内容

[0005] 针对上述问题,本发明提出了一种用于RFID的限定距离的安全认证协议。

[0006] 为实现上述目的,本发明采用如下技术方案:

[0007] 一种用于RFID的限定距离的安全认证协议,包括:

[0008] 初始化:生成阅读器与标签的公私钥,在阅读器中存储阅读器的私钥与标签的公钥,在标签中存储标签的私钥与阅读器的公钥;通过阅读器确定最大限定距离;

[0009] 阅读器认证标签:标签发起认证请求并发送一个随机数给阅读器,阅读器回应一个随机数给标签;标签与阅读器通过各自的私钥,对方的公钥以及接收到的随机数计算认证值;同时标签与阅读器间进行n轮时序严格的会话,用来验证限定距离;阅读器接收并检验标签计算的认证值是否合法,同时检验标签的距离是否有效,若通过,则认证通过,否则认证失败。

[0010] 进一步的,所述生成阅读器与标签的公私钥的具体方法为:

[0011] 根据安全参数1,发行者选取对应的椭圆曲线群G与模为p的整环Zp,从Zp中随机选取一个y作为阅读器的私钥,并计算Y=yP作为阅读器的公钥;从Zp中随机选取一个x作为标签的私钥,并计算X=xP作为标签的公钥;将x,Y秘密发送给标签,将y,X秘密发送给阅读器;其中,G的阶为p,生成元为P。

[0012] 进一步的,通过阅读器确定最大限定距离的具体方法为:

[0013] 根据安全参数1,阅读器确定一个合法标签与自己之间的最大距离 \in ;同时根据 \in 与系统参数,阅读器确定进行通讯的最大轮数n和一轮通信所需的最大时间 Δt 。

[0014] 进一步的,阅读器认证标签的具体方法为:

[0015] a.标签从Zp中随机选取一个r1,并计算R1=r1P,标签将R1发送给阅读器;阅读器从Zp中随机选取一个r2,并计算R2=r2P,阅读器将R2发送给标签;

[0016] b.标签首先计算L=r1Y+xR2 $\in G$,因为R1,R2,L $\in G$,且G是基于椭圆曲线的循环群,所以R1,R2和L是椭圆曲线上的点,因此,标签得到L的横坐标值,用xcoord(L)来表示;标签取xcoord(L)的前2n位,用[xcoord(L)]_{2n}来表示;最后标签将[xcoord(L)]_{2n}的前n位赋值给t⁰,将[xcoord(L)]_{2n}的后n位赋值给t¹;

[0017] c.阅读器计算[xcoord(yR1+r2X)]_{2n},并将[xcoord(yR1+r2X)]_{2n}的前n位赋值给 \tilde{t}^0 ,将[xcoord(yR1+r2X)]_{2n}的后n位赋值给 \tilde{t}^1 ;阅读器从Zp中随机选取一个e',并根据通讯轮数n,首先将e'使用一个哈希函数映射为长度为n的比特串,即 $e = f(e')$;其中 $f(\cdot) : \{0, 1\}^* \rightarrow \{0, 1\}^n$ 是一个映射到n比特的哈希函数;随后阅读器将e分为n比特,其中第i比特我们用(e)_i($i \in [1, n]$)来表示,令c_i=(e)_i;

[0018] d.阅读器与标签开始n轮时序严格的会话,具体为:阅读器将c₁至c_n依次发送给标签,并且在发送c₁时开始计时;每次当标签收到c_i($i \in [1, n]$)后,存储c_i,计算f_i=(1-c_i)(t⁰)_i+c_i(t¹)_i,并将f_i发送给阅读器,其中(t⁰)_i代表t⁰的第i比特,(t¹)_i代表t¹的第i比特;阅读器收到f_i后,计算f_i*=(1-c_i)(\tilde{t}^0)_i+c_i(\tilde{t}^1)_i,并验证等式f_i*=f_i是否成立;若对于i $\in [1, n]$,任意一个i时,等式f_i*=f_i不成立,则认证失败;否则,在验证完成f_n*=f_n后,进行下一轮会话;任意一个i时,会话完成时停止计时,并在第i+1次会话开始时重新计时;设第i轮会话共需时间为 τ_i ($1 \leq i \leq n$);

[0019] e.阅读器将e发送给标签;标签收到e后,验证c₁||c₂||…||c_n=e是否成立;若成立,标签将t⁰||t¹发送给阅读器;

[0020] f.阅读器首先验证等式 $\tilde{t}^0 \parallel \tilde{t}^1 = t^0 \parallel t^1$ 是否成立,若不成立,则认证失败;否则,阅读器验证 $\tau_i \leq \Delta t$ ($1 \leq i \leq n$)是否成立,若不成立,则认证失败;否则,认证成功。

[0021] 本发明的有益效果为,与传统的适用于RFID系统中的认证协议相比,本发明除了能够使得阅读器对标签的身份进行认证,还能对标签与阅读器之间的距离进行认证;一个

合法用户在限定距离之外,不能通过阅读器的认证。

具体实施方式

[0022] 下面结合详细描述本发明的技术方案:

[0023] 系统初始化:

[0024] 发行者根据安全参数1,发行者选取对应的椭圆曲线群G与模为p的整环Zp,从Zp中随机选取一个y作为阅读器的私钥,并计算Y=yP作为阅读器的公钥;从Zp中随机选取一个x作为标签的私钥,并计算X=xP作为标签的公钥;将x,Y秘密发送给标签,将y,X秘密发送给阅读器;其中,G的阶为p,生成元为P;

[0025] 阅读器的初始化:根据安全参数1,阅读器确定一个合法标签与自己之间的最大距离 \in ;同时根据 \in 与系统参数,阅读器确定进行通讯的最大轮数n和一轮通信所需的最大时间 Δt 。

[0026] 阅读器认证标签的具体方法为:

[0027] a. 标签从Zp中随机选取一个r1,并计算R1=r1P,标签将R1发送给阅读器;阅读器从Zp中随机选取一个r2,并计算R2=r2P,阅读器将R_2发送给标签;

[0028] b. 标签首先计算L=r1Y+xR2 \in G,因为R1,R2,L \in G,且G是基于椭圆曲线的循环群,所以R1,R2和L是椭圆曲线上的点,因此,标签得到L的横坐标值,用xcoord(L)来表示;标签取xcoord(L)的前2n位,用[xcoord(L)]_{2n}来表示;最后标签将[xcoord(L)]_{2n}的前n位赋值给t⁰,将[xcoord(L)]_{2n}的后n位赋值给t¹;

[0029] c. 阅读器计算[xcoord(yR1+r2X)]_{2n},并将[xcoord(yR1+r2X)]_{2n}的前n位赋值给t̃⁰,将[xcoord(yR1+r2X)]_{2n}的后n位赋值给t̃¹;阅读器从Zp中随机选取一个e',并根据通讯轮数n,首先将e'使用一个哈希函数映射为长度为n的比特串,即e=f(e');其中f(•):{0,1}*→{0,1}ⁿ是一个映射到n比特的哈希函数;随后阅读器将e分为n比特,其中第i比特我们用(e)_i(i \in [1,n])来表示,令c_i=(e)_i;

[0030] d. 阅读器与标签开始n轮时序严格的会话,具体为:阅读器将c₁至c_n依次发送给标签,并且在发送c₁时开始计时;每次当标签收到c_i(i \in [1,n])后,存储c_i,计算f_i=(1-c_i)(t⁰)_i+c_i(t¹)_i,并将f_i发送给阅读器,其中(t⁰)_i代表t⁰的第i比特,(t¹)_i代表t¹的第i比特;阅读器收到f_i后,计算f_i*=(1-c_i)(t̃⁰)_i+c_i(t̃¹)_i,并验证等式f_i*=f_i是否成立;若对于i \in [1,n],任意一个i时,等式f_i*=f_i不成立,则认证失败;否则,在验证完成f_n*=f_n后,进行下一轮会话;任意一个i时,会话完成时停止计时,并在第i+1次会话开始时重新计时;设第i轮会话共需时间为τ_i(1≤i≤n);

[0031] e. 阅读器将e发送给标签;标签收到e后,验证c₁||c₂||…||c_n=e是否成立;若成立,标签将t⁰||t¹发送给阅读器;

[0032] f. 阅读器首先验证等式t̃⁰||t̃¹=t⁰||t¹是否成立,若不成立,则认证失败;否则,阅读器验证τ_i≤Δt(1≤i≤n)是否成立,若不成立,则认证失败;否则,认证成功。

[0033] 本发明所述的协议可以抵抗伪造攻击、冒充攻击、中间人攻击、重放攻击和距离伪装欺骗。亦即,在本发明所述的协议中,任何一个敌手不能通过伪造标签的信息来欺骗阅读器;任何一个敌手不能通过拦截标签的会话信息来冒充一个合法标签欺骗阅读器;任何一

个敌手不能通过截获与篡改标签与阅读器之间的会话信息来使认证协议失效；任何一个敌手不能通过重放一个合法标签在先前进行认证时与阅读器的交互信息来欺骗阅读器；任何一个敌手不能够在限定距离之外通过阅读器的认证。与此同时，本发明的协议能够提供对外部敌手的匿名性，在标签与阅读器进行认证的过程中，任何一个外部敌手都不能够通过截获标签与阅读器的交互信息来确定标签的身份，这在很大程度上保证了标签的隐私信息。