

基于 WPKI 技术的安全移动支付系统研究

韩景灵,张秀英

(山西大学 商务学院,山西 太原 030031)

摘要: 为了有效解决移动支付信息安全问题,在分析和研究无线应用协议(WAP)、公开密钥基础设施(WPKI)和移动网络安全威胁的基础上,提出了一种基于 WAP 和 WPKI 技术的移动支付安全解决方案。该方案通过对 WAP 和 WPKI 体系结构和优化性的分析,确定了基于 WAP 和 WPKI 的移动支付体系结构模型,并对安全支付系统功能模块进行了详细的设计。通过分析表明,该解决方案可为移动支付提供加密、认证等安全服务,为移动网络中的安全支付提供了较好的安全保障。

关键词: 移动支付;WAP;WPKI;认证中心;身份认证

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2014)06-0156-05

doi:10.3969/j.issn.1673-629X.2014.06.039

Research on Mobile Safe Payment System Based on WPKI

HAN Jing-ling, ZHANG Xiu-ying

(Business College of Shanxi University, Taiyuan 030031, China)

Abstract: To solve the information security problem of mobile payment effectively, based on analysis of WAP, WPKI technology and risk of mobile net, a security scheme of mobile payment based on WAP and WPKI technology is presented. A structure of mobile payment is constructed based on WAP and WPKI through analyzing system structure and optimization performance of WAP and WPKI. Moreover, the design is focused on function block of the security platform. The analysis shows that the security scheme provides security needs of mobile payment such as confidentiality, authentication and improve security of payment on wireless net.

Key words: mobile payment; Wireless Application Protocol (WAP); Wireless Public Key Infrastructure (WPKI); Certificate Authority (CA); identity authentication

0 引言

近些年来,随着计算机技术与无线通信技术的发展,以及移动通信技术同传统网络应用的结合,使得移动设备可以通过无线网络接入 Internet,从而产生了新的商务交易模式和办公模式。移动支付作为一种新型的支付方式,得到了广泛的应用。与此同时,由于移动支付要经过运营商的无线网络接入,以及信息在空中的无线传播,这就有可能发生信息泄密或引入黑客攻击的问题。移动网络同传统网络相比,其安全性更加脆弱,同时对安全性的要求更高。因此如何保护移动支付和信息的安全,成为移动支付使用和推广的首要问题。文中探讨并研究分析了 WAP 和 WPKI 平台的各个实现方面,研究了 WAP 协议的安全特点和 WPKI 技术的安全特点,并在综合各种技术的基础上,根据将

来国内 3G 网络环境的特点和终端的性能特点等应用环境,给出了一套基于 WAP 和 WPKI 技术的整体实现方案,使得研究的体系具有保密性、完整性、身份认证和不可否认性。

1 WAP 协议体系结构

1.1 WAP 协议简介

WAP^[1] (Wireless Application Protocol) 为无线应用协议,是一项全球性的网络通信协议,是一种开放的全球标准。借助 WAP,用户可以使用手机、掌上电脑等无线终端,通过 WAP 接入 Internet,将 Internet 的信息和业务引入到移动电话 PALM 等无线终端中。WAP 能够运行在各种无线网络中,无论在何时何地,只要在手机中安装了微型浏览器,就可以随时随地享受网上

收稿日期:2013-07-28

修回日期:2013-11-06

网络出版时间:2014-02-24

基金项目:山西省软科学研究计划项目(2011041018-04)

作者简介:韩景灵(1981-),女,山西太原人,硕士,讲师,研究方向为计算机安全、电子商务安全、移动电子商务安全;张秀英,硕士,副教授,研究方向为网络营销、电子商务。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20140224.0857.009.html>

信息或网上资源。WAP 支持 WML (Wireless Markup Language, 无线标注语言), 因为 WML 才是专门为小屏幕和无线键盘手持设备服务的语言, WAP 把 Internet 上用 HTML 语言描述的信息转换成了用 WML 描述的信息, 显示在移动设备的显示屏上。

1.2 WAP 模型

WAP 模型^[2]由具有用户代理的移动设备、WAP 网关和 WAP 服务器三部分构成, 其模型如图 1 所示。

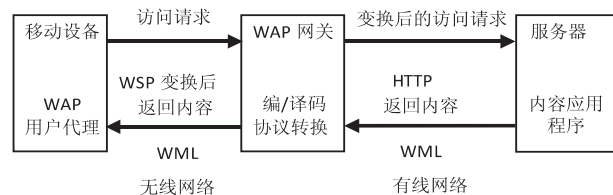


图 1 WAP 的模型

WAP 网关^[3], 又称为 WAP 代理, 是 WAP 的应用模型中的核心内容, 它起着协议的“翻译”作用, 同时还连接着无线网络与 Internet, 实现了 WAP 协议与因特网协议的相互转化, 是无线网络与万维网的桥梁。同时为移动终端访问传统网络中的资源提供路由支持, 通过 WAP 网关能够保证移动用户连接到 Internet, 享受各种各样的网上信息或者网上资源。用户利用 WAP 访问 Internet 的具体过程如下:

(1) 当移动用户想要浏览因特网上的信息时, 用户可以从 WAP 移动设备终端输入所要访问的 WAP 服务器的地址, 信号通过无线网络后, 把访问请求发送到 WAP 网关, 用户代理先与 WAP 网关建立连接;

(2) WAP 网关通过协议转换, 以 HTTP 协议方式通过有线网络将用户请求发送至因特网服务器;

(3) 因特网服务器以 HTTP 协议方式与 WAP 网关进行交互, 将生成的结果送回给 WAP 网关;

(4) 最后 WAP 网关将内容经过解码、编码以及压缩后, 处理成二进制送回移动终端设备, 并显示在客户的 WAP 移动终端上。

1.3 WAP 的安全架构

WAP^[4]是由 WMLScript (无线标记语言脚本)、WPKI (无线公钥基础设施)、WIM (无线鉴别模块)^[5]和 WTLS (无线传输层安全) 四部分组成的。其安全架构如图 2 所示。

每个部分都各自承担不同的作用。WPKI 即“无线公钥基础设施”, 它是一种密钥管理平台。作为一种安全基础设施的平台, WPKI 可以管理在移动无线网络环境中使用的公开密钥和数字证书, 同时, 在 WAP 安全架构中, 它还可与 WTLS、TCP/IP、WML 相互结合, 为各个参与的部分提供数字证书的发放及审核等管理, 提供加密、数字签名、身份认证和不可抵赖性的功能, 从而建立安全的无线网络环境, 解决移动支付

的安全问题。

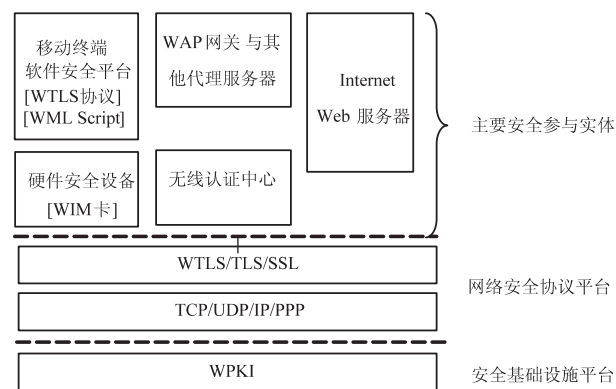


图 2 基于 WAP 的安全架构

网络安全协议平台包括 WTLS 协议、位于传输层上的安全协议 TLS (有线环境下)、SSL^[6]和 TCP/IP 协议。WAP 规范的协议栈中专门设有一个安全协议层, 即无线安全传输层协议 (WTLS)。WTLS^[7]是 WPKI 的安全保障核心, 它将 Internet 的安全扩展到了无线环境, 适合在窄带通信信道上使用。WTLS 为了适应无线网络较低的数据传输率, 并考虑到了目前手机等无线装置的运算能力与内存限制问题, 对 TLS 进行了一定程度的改进。WTLS 处于传输层之上的安全层, 是 WAP 协议栈的可选层, 是模块化的。它的功能类似有线网络当中的 SSL 加密传输协议, 它的作用主要是保障 WAP 设备和 WAP 网关之间的安全性, 除了对内容在传输的过程中进行安全保密外, 还可认证参加通信的各方, 并检查其完整性。并且 WTLS 可以检测并拒绝重放数据, 对于没有通过验证的数据也将拒绝服务。

主要安全参与实体包括移动终端安全平台, 硬件安全设备, WAP 网关及代理服务器, 无线认证中心及 Internet Web 服务器。其中 WMLScript^[8]是一种能够提供编程功能的轻量级语言, 类似于 JavaScript 和 ECMAScript。它是一种无线标记语言, 从 HTML 继承而来, 但与 HTML 相比, 浏览器消耗的内存和 CPU 时间更少, 因此, WML 更适合移动电话等手持移动设备。WIM (WAP Identity Module) 是 WAP 的身份识别模块, 是在 SIM 卡上的一个安全模块, 可以将这两张卡结合在一起。WIM 卡是可防篡改的芯片设备, 可以在其中存储用户的私钥。有效防止密钥的泄漏。除保存私钥外, WIM 卡还可以访问密钥、证书、认证对象。WIM 为 WAP 提供了加密操作, 还负责存储数字证书及数字证书的验证。

2 WPKI 技术

2.1 WPKI 技术简介

无线公钥基础设施 (Wireless Public Key Infrastructure, WPKI)^[9]是一种遵循既定标准的密钥管理平台。

WPKI 并不是一个全新的标准,而是将传统有线环境中的 PKI 技术进行了优化扩展,应用在了无线环境中。因为 PKI^[10] 技术在无线环境中应用非常困难,并且对系统的要求很高,故而 WPKI 在 PKI 的基础上进行了一定改进、优化及扩展,来适应无线网络带宽窄、无线设备计算能力低等特点。WPKI 具有完善的密钥和证书管理体系,WPKI 最关注的是政策和标准以用来管理电子商务,并在无线应用环境下通过 WTLS 和 WMLScript 来提供安全服务,它能够满足移动电子商务的安全要求,即保密性、完整性、真实性和不可抵赖性。WPKI 采用了优化的 ECC^[11] 算法和压缩的 X.509 数字证书,通过认证中心(CA)这个第三方的可信任机构来验证用户的身份,从而实现信息在无线网络中的安全传输,降低了交易的风险。

2.2 WPKI 系统组成和原理

WPKI 的主要组件包括终端实体应用程序、PKI Portal^[12]、认证中心(CA)、目录服务器(PKI Directory)、WAP 网关与有线服务器等设备。

终端实体应用程序是指支持 WAP 应用的移动设备,例如 WAP 手机、支持 WAP 的 PDA 等。它包含 SIM 卡和 WIM 卡,或者将这两种卡合二为一的 SWIM 卡。该卡将具有存储、加密及数据处理能力的集成电路芯片镶嵌其中,卡片装载着持卡人、服务器的数字证书,私钥及加密签名模块,从而实现移动电子商务中的信息加密传输、身份认证和数字签名等功能。在 WPKI 中,PKI Portal 给用户和 CA 提供一个借口,用来代替有线网络中 RA(Registration Authority)^[13] 的功能。它接受用户的证书签名请求,确认用户的身份,并负责把用户的需求转发给 CA(Certification Authority)提出证书请求。PKI Portal 内嵌 RA 函数,能在无线客户设备和有线的服务器中转换 PKI 消息格式,与有线网络中的 CA 进行交互;CA 是 WPKI 的信任基础,主要负责生成、颁发和验证数字证书,规定证书有效期和刷新证书等证书的管理;WAP 网关负责处理终端用户与有线服务器之间的协议转换工作;目录服务器用于提供用户身份信息和证书查询,存储已签发的数字证书,保留最新的证书撤销列表(CRL),用户可查询验证,获得所需的用户的证书及公钥;WTLS 主要负责保证传输层的安全,它是由传统有线网络的 TLS 协议改进和优化而得来的。WPKI 的基本结构和数据流向如图 3 所示。

一次完整的 WPKI 操作流程有:

(1) 移动终端用户向 PKI 入口提交用户信息、证书申请、证书注销、更新申请等请求;

(2) PKI Portal 对用户的申请进行审查,审查合格且确认用户的 ID 后,向 CA 进行证书请求;

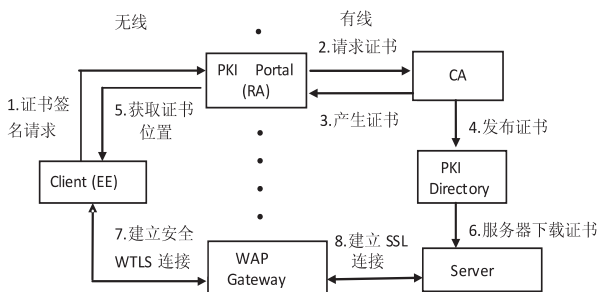


图 3 WPKI 数据业务流程模型

(3) CA 将生成的服务器证书、用户要恢复的密钥、移动终端证书的 URL 等交给 PKI Portal;

(4) CA 同时将生成的用户的公钥证书发布到目录服务器中,供其他用户查询、下载;

(5) PKI 入口向移动终端提供用户要恢复的密钥以及保存移动终端用户的证书,发送移动终端证书的 URL,这个证书 URL 就是证书在目录服务器中的地址;

(6) 网络服务器可以向目录服务器提交查询证书请求,目录服务器将用户证书的 URL 交给有线网络服务器;

(7) 通过 CA 颁发的证书,移动终端和 WAP 网关之间建立安全的 WTLS 连接;

(8) 通过传统网络,WAP 网关将移动终端的请求信息发送给有线网络服务器,有线网络服务器可以将信息返回给移动终端。从而,WAP 网关与有线网络服务器之间建立了 SSL 连接。

移动终端用户通过 PKI 入口向 CA 申请数字证书,CA 审核移动终端用户身份后,将数字证书签发给用户,移动终端用户将数字证书、私钥等信息存放在智能卡中。如果服务器需要验证用户的证书,用户将发送自己证书的 URL 给服务器,服务器根据 URL 到目录服务器上下载用户证书;如果用户需要验证服务器的证书,服务器将证书通过下载存储到用户的移动终端。

3 基于 WAP 和 WPKI 的移动支付系统的设计

随着网络技术和无线电信息技术的不断发展,移动电子商务越来越得到人们的青睐。移动支付方式的安全性显得尤为重要。

3.1 设计方案的基本要求

在整个移动支付的过程中,涉及到的参与者包括:

- (1) 买方:参与交易的消费者;
- (2) 卖方:交易中的产品或服务提供者;
- (3) 移动运营商:提供无线网络的支持;
- (4) 银行:提供转账等银行相关服务;

(5)第三方服务提供商:提供与支付相关的平台服务。

各方之间必须相互交换买方和卖方的签名私钥,加密信息的公钥及与付款相关的商业信息。这些机密信息一旦被黑客截获,会产生交易者身份被假冒,敏感信息被盗取或篡改,交易参与者对进行过的交易抵赖等风险,将会给整个移动支付系统的安全性带来致命的危害。

为了避免移动支付的交易风险,一个安全的交易系统应该具备以下的特性:

- 身份认证:即确保交易过程中参与交易的各方的身份是互相可以认证、信任的,以防止欺诈行为的发生。
- 保密性:即确保在交易过程中只有交易的双方才能知道交易的隐私数据,防止隐私数据为非法用户所获得。
- 完整性:即确保交易过程中的相关信息及数据不会被窃听者截获并修改,且交易各方可以辨别信息的真实性,一旦被篡改,交易终止。
- 不可否认性:即确保交易行为一旦完成,参与交易的各方对曾经进行过的交易行为不能否认、抵赖。

3.2 方案概述

3.2.1 各模块间的网络拓扑

现在,文中就基于 WAP 和 WPKI 技术来设计一个安全的移动支付系统。结合实际情况,在移动支付的过程中,会涉及到两种不同的网络。

第一种是无线网络,它由通信运营商提供。客户使用移动终端(主要是智能手机)通过无线网络的网关和系统的其他部分相连。对移动终端的要求是:需要具有一定的处理能力,支持 WAP 应用,支持 WTLS 等技术,以此来完成在移动支付过程中移动终端和无线 WAP 网关之间需要建立的安全通道,将协商出的密钥对信息加密,实现信息保密性、发送以及签名功能。

第二种是有线网络。除了支付者之外,系统的其他组成部分之间都要通过有线网络连接。有线网络与无线网络相比,带宽更高,处理能力更强,使用的协议也更加复杂(如 SSL 密码协议),安全性也更高。

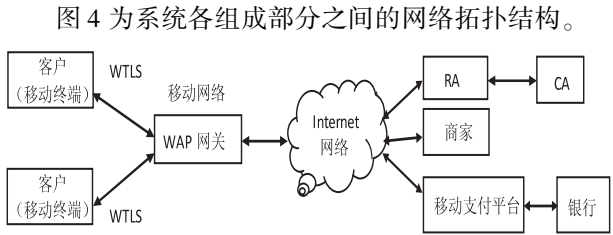


图4 移动支付各组成部分之间的网络拓扑

该移动支付系统以 WPKI 为基础,依据移动支付业务需求设计,各模块功能如下:

(1)RA 服务器负责完成用户信息和用户申请信息的管理,为用户提供申请证书时用户身份的检查 and 审核,以及消息的通知,同时用户也可以向 RA 进行证书的注销申请及更新申请,并将申请提交给 CA 服务器;

(2)CA 是整个安全系统的基础和核心,CA 服务器主要负责完成密钥的产生、备份和管理,提供证书目录和证书的生成、发放、注销、更新,并发布证书注销列表(CRL)等功能;

(3)商家提供客户所需的商品或某种服务,为用户提供商品浏览和定购,来完成商品的交易;

(4)移动支付平台提供与银行的接口,主要负责完成对支付者及商家身份的认证,以及对商家及客户的账户管理,实现二者之间的转账。在支付中,移动支付平台提供与客户、商家的支付接口,进行信息交互。

3.2.2 系统组成和各模块功能

文中设计的移动支付解决方案包括 5 个模块:商家、客户、银行系统、认证中心(CA)和交易中心(第三方信任实体)。该方案各个组成部分的模型结构如图 5 所示。

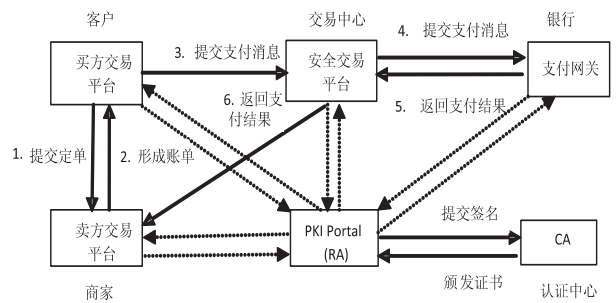


图5 移动支付体系安全方案模型图

其中,客户是通过手机完成支付的消费者,客户和商家完成定单及账单的提交和生成。买方交易平台获得证书后配置客户服务器证书,一方面提供产品订购过程中的安全功能:与卖方交易平台之间进行相互的身份识别,对与商家之间传递的商业信息进行加、解密,生成客户对定单的数字签名,验证商家对账单的承诺;另一方面实现支付过程中的安全功能:与交易中心之间相互的身份识别,采用银行的公钥对提交的转账信息进行消息加密,生成交易证据的数字签名,生成交易中心的交易证据,供日后查询。

卖方交易平台为客户提供商品或服务,通过交易中心完成商品的交易,同时在交易完成后对客户进行信用评价。卖方交易平台获得证书后配置商家服务器证书,一方面提供商品订购过程中的安全功能:与买方交易平台(客户)之间进行相互的身份识别认证,对于客户之间传递的商业信息进行加、解密,对客户定单的数字签名进行验证,并且生成商家对账单和承诺的数

字签名;另一方面提供支付过程中的安全功能:与交易中心之间相互的身份识别认证,对银行返回的支付结果的数字签名进行验证。此外,卖方交易平台还记录客户签名后的定单信息、支付信息以及送货信息等。

安全交易平台配置交易中心的服务器证书,用于与卖方交易平台、买方交易平台、银行系统之间的相互的身份识别、消息加密和生成数字签名,对客户提交的交易证据的数字签名进行验证,对银行响应的支付结果的数字签名进行验证,对交易过程中传输的交易数据、支付历史数据等重要信息进行存储,为日后产生争议时提供解决的证据,并验证争议各方提交证据的真伪性。

银行系统配置商业银行的服务器证书,提供了与安全交易平台之间联系的公共接口,主要完成支付网关的功能,负责处理支付信息。银行系统提供与安全交易平台之间的相互的身份识别,完成银行系统与互联网及移动网络之间的通讯、协议的转换以及数据的加解密功能;同时,对客户的数字签名进行验证,对客户传来的转帐信息进行解密,将支付的结果信息与产生的支付结果的数字签名传递给商家。其中,支付结果用商家的公钥来加密。此外,银行系统还对支付的历史数据进行存储管理,提供密钥与证书的管理等服务。

CA 和 PKI Portal(RA)用来保证系统的安全性;各参与实体(包括买方交易平台、卖方交易平台、安全交易平台和银行系统)所使用的公钥由 CA 签发的证书来分配。各参与实体使用生成密钥对和证书请求,向 RA 申请证书,RA 在完成对各个参与实体的身份审核后向 CA 提出证书签发申请,CA 签发证书后并通过证书库进行发布,然后 CA 将用户证书回送给 RA,RA 将证书回送给各参与实体,存放在各自的模块当中。

3.2.3 安全方案的交易流程

图 5 中虚线代表 CA 分别向商家、客户、安全交易平台和银行系统颁发身份认证证书,实线代表移动支付解决方案的交易过程。交易过程共有六个具体步骤,其主要描述如下:

(1)客户使用手机终端浏览器,通过 WAP 网关浏览商家的服务器,选择所需的商品进行订购。客户用商家签名公钥验证其签名,若通过,根据商家的要求向商家提交定单,将商品信息、用户编号、交货地址等信息加密后发给商家;

(2)商家收到购买信息后,形成相应的账单并产生惟一的定单号。然后将账单信息、商家的说明及承诺发到客户手机浏览器;

(3)客户用自己的交易私钥对支付合同用签名算法进行签名,把签名信息等支付消息提交到安全交易

平台;

(4)安全交易平台收到客户的支付消息后,从 CA 下载客户的数字证书,对签名进行验证,若验证成功,则说明该支付信息确实由支付者发出,将支付消息转发到银行系统;

(5)银行对客户支付消息的数字签名进行验证,并且取出支付指令,进行转账,转账信息必须包括支付者账户号码和商家账户号码;并将支付是否成功、支付的金额等支付结果告知安全交易平台,交易平台将支付状态记录保存,作为支付凭证;

(6)最后安全交易平台将支付结果实时告知商家。

4 系统安全性分析

(1)保密性方面,在无线网络的通信采用了 WTLS 握手协议,而在有线网络中,通信则采用了传统的 SSL 密码协议,这样在系统各模块间的信息通道都是安全的。作为商家,他只知道客户选购商品的信息,而对客户的身份信息及账号信息等隐私却不知道;而作为银行系统,他只知道客户的账户信息,而不知道客户购买商品的信息。交易中各方各环节中,都使用密钥对传送的敏感信息进行加密,参与交易的各方只知道自己该知道的信息,这样保证了敏感信息的私密性。

(2)身份认证方面,系统中参与交易的各方所使用的证书均由 CA 来签发分配,发送方利用其私钥对数据进行签名,而接收方利用证书中的公钥信息对签名信息进行验证,从而实现了交易各方相互间的身份真实性的认证。

(3)不可否认性方面,系统利用交易的各方中发送方的私钥来做签名,用接收方的公钥来解密并验证,这就保证了只有交易的双方能够对数据进行签名工作;另外,系统的安全交易平台记录保存了每个环节的历史数据及支付信息,使得支付者不能对签名进行抵赖。从而也保证了事后对交易的不可抵赖性。

5 结束语

该安全移动支付系统使用了 WAP 环境中 WTLS 协议来保证无线环境中与第三方建立安全的支付方式。各参与实体所使用的数字证书及公钥均由 CA 签发的证书来分配,可以充分保障移动电子商务支付的机密性、认证性、公平性和完整性。综上所述,该移动支付方案能满足用户在安全性能方面的各个需求。随着网络技术的发展,网络传输速度的不断提高,用户对移动支付方式的安全需求将更加严格,如何改善移动支付的协议,改进移动支付平台以适应用户的需求,将

(下转第 165 页)

较大差异,而且新的破坏事件也会不断涌现。因此文中的分类器无论选择是基于BP还是基于RBF的人工神经网络都没有办法使用样本库以外的信号学习、训练,这个限制抑制了系统的应用区域,因此,需要在进一步的研究中为系统的分类器建立增量学习机制,即将预警信号的校验结果反馈给环境感知机制,自动监督训练信号分类器与事件分析参数。同时由于文中研究得到入侵事件信号的种类有限,在使用人工神经网络中,只建立了人员行动这一入侵事件的样本库,所以现今的系统还只能识别人员行动这一入侵事件。在后续研究中,需要进一步扩展人工神经网络的样本库,使得信号分类能做到更精细和更准确。

参考文献:

[1] Kersey A D. A review of recent developments in fiber optic sensor technology[J]. Optical Fiber Technology,1996,2(3):291-317.

[2] Katsifolis J, McIntosh L. Apparatus and method for using a counter-propagating signal method for locating events;U. S. , 7499177[P]. 2009.

[3] de Vries J. A low cost fence impact classification system with neural networks[C]//Proceedings of 7th AFRICON conference in Africa. Gaborone:[s. n.],2004:131-136.

[4] Min Hwang-Ki, Lee Chung-Yeo, Lee Jong-Seok, et al. Abnormal signal detection in gas pipes using neural networks [C]//Proceeding of 33rd annual conference of the IEEE industrial electronics society. Taipei:IEEE,2007:2503-2508.

[5] Mahmoud S S, Katsifolis J. Robust event classification for a fiber optic perimeter intrusion detection system using level

crossing features and artificial neural networks [C]//Proc of SPIE. [s. l.]:[s. n.],2010.

[6] Mahmoud S S, Visagathilagar Y, Katsifolis J. Real-time distributed fiber optic sensor for security systems: performance, event classification and nuisance mitigation[J]. Photonic Sensors,2012,2(3):225-236.

[7] Jiang Lihui, Liu Xiangming, Zhang Feng. Multi-target recognition used in airport fiber fence warning system[C]//Proceedings of 2010 international conference on machine learning and cybernetics. Qingdao:[s. n.],2010:1126-1129.

[8] 饶云江,吴敏,冉曾令,等. 基于准分布式FBG传感器的光纤入侵报警系统[J]. 传感技术学报,2007,20(5):45-49.

[9] 陶沛琳,延凤平,刘鹏,等. 基于Mach-Zehnder干涉仪的光纤入侵行为识别系统[J]. 量子电子学报,2011,28(2):183-190.

[10] 赵杰,丁吉,万遂人,等. 全光纤安防系统模式识别混合编程的实现[J]. 东南大学学报(自然科学版),2011,41(1):41-46.

[11] 王立. 基于分布式光纤传感的智能环境感知技术研究[D]. 天津:南开大学,2008.

[12] Cho D, Bui T D, Chen G. Image denoising based on wavelet shrinkage using neighbor and level dependency[J]. International Journal of Wavelets, Multiresolution and Information Processing,2009,7(3):299-311.

[13] Nason G P, Silverman B W. The stationary wavelet transform and some statistical applications[M]//Wavelets and Statistics. New York:Springer,1995.

[14] 飞思科技产品研发中心. 人工神经网络理论与MATLAB实现[M]. 北京:电子工业出版社,2005.

(上接第160页)

会成为一个越来越重要的研究方向。

参考文献:

[1] Wireless Application Protocol Forum, Ltd. WAP 无线应用协议[M]. 北京:机械工业出版社,2000.

[2] 张慧媛,李晓峰,杨放春. 移动互联网与WAP技术[M]. 北京:电子工业出版社,2002.

[3] 胡晓军. WAP网关的研究与实现[D]. 杭州:浙江大学,2005.

[4] 吴冬梅. WAP中的安全构架模型研究[J]. 电力系统通信,2004(6):50-52.

[5] Wireless Application Protocol Forum, Ltd. Wireless identity module specification[EB/OL]. 2006. <http://technical.openmobilealliance.org/Technical/wapindex.aspx>.

[6] Davies J. Implementing SSL/TLS using cryptography and PKI [M]. USA:Wiley,2011.

[7] 袁志锋,刘广东,朱琦. 基于WTLS的WAP安全实现研究[J]. 信息技术,2004,28(12):62-64.

[8] 赵晓枫. 精通WAP/WML[M]. 北京:科学出版社,2001.

[9] 马建锋,朱建明. 无线局域网安全-方法与技术[M]. 北京:机械工业出版社,2005.

[10] 王建兵. PKI数字证书在WEB系统中的安全应用[J]. 国土资源信息化,2005(1):40-44.

[11] Sun Hung-Min. Cryptanalysis of Aydosetal's ECC-based wireless authentication protocol[C]//Proceedings of the 2004 IEEE international conference on e-technology, e-commerce and e-commerce and e-service. [s. l.]:IEEE Computer Society,2004.

[12] 徐晓宁. WPKI关键技术的设计与实现[D]. 西安:西安电子科技大学,2005.

[13] 王保明. 证书认证系统设计与实现[D]. 济南:山东大学,2009.

基于WPKI技术的安全移动支付系统研究

作者：[韩景灵](#)，[张秀英](#)，[HAN Jing-ling](#)，[ZHANG Xiu-ying](#)

作者单位：[山西大学 商务学院, 山西 太原, 030031](#)

刊名：[计算机技术与发展](#)

英文刊名：[Computer Technology and Development](#)

年，卷(期)：2014 (6)

本文链接：http://d.wanfangdata.com.cn/Periodical_wjfz201406039.aspx