基于包延时的安全标记与数据流绑定方法*

冯 瑜, 杜学绘, 曹利峰
(解放军信息工程大学 数学工程与先进计算国家重点实验室, 郑州 450004)

摘 要: 提出了一个独立于数据包内容的安全标记与数据流绑定方法,该方法基于包延时调制,引入数据包的到达间隔时延为安全标记的载体,使用海明码实现安全标记的差错控制,设计数据包随机分组方式,并根据绑定规则调制数据包延迟时间,实现了安全标记与数据流的隐式绑定,解决了显式安全标记绑定引起的针对性攻击和灵活性不足等问题。理论分析和实验结果表明,该绑定方法对网络随机时间扰乱具有健壮性,能保证网络传输中安全标记的安全性。

关键词: 安全标记; 绑定; 数据流; 包延时
中图分类号: TP393.08 **文献标志码**: A **文章编号**: 1001-3695(2014)02-0571-05
doi:10.3969/j.issn.1001-3695.2014.02.060

Packet delay based binding method of label to data stream

FENG Yu, DU Xue-hui, CAO Li-feng
(*State Key Laboratory of Mathematical-Engineering & Advanced Computing*, *PLA Information Engineering University*, *Zhengzhou* 450004, *China*)

Abstract: This paper proposed a labeling to data stream binding method independent of the contents of the packet, which based on packet delay modulation, and introducing the packet inter-arrival delay as the new labeling vector. The method used Himming code to achieve the label error control, designing the data packet randomized blocks, and modulated the packet delay time according to the label binding rules, then realized the implicit binding of security label to data stream. Based on this method, it solved the targeted attack problems caused by explicit binding method and its inflexibility. Theoretical analysis and experimental results demonstrate that the proposed method is robust against the network random timing perturbation and safety the binding security label when is transmitted in the network.

Key words: security label; binding; data stream; packet delay

安全标记是多级安全的基础,构建多级安全网络要求实现基于安全标记的访问控制保护与数据安全传输功能。如何将安全标记与客体进行绑定,成为构建多级安全网络,影响多级安全实施有效性和灵活性的关键。多级安全网络中安全标记的绑定包括与系统中数据客体以及网络传输数据流的绑定。通常安全标记与数据客体的绑定主要包括在客体中写入标记[1,2]和逻辑维护[3~5]两种方法。标记写入的绑定方法是通过在客体中包含标记来实现的,如电子邮件的第一行、文件的头部或尾部[6];逻辑维护主要通过链表、数据库等方式建立数据客体与安全标记的关联关系,完成标记到客体的绑定。这两种绑定方式前者主要应用于操作系统中,后者不能实现标记跟随数据流,都不适用于多级安全网络环境。

为支持多级安全网络环境下基于安全标记的数据流多级安全控制,国际上制定了一系列规范标准。美国军方于 1991 年提出了 IPSO(IP security option)携带安全标记的方法,采用在 IP 头选项字段(IP 头后 20 Byte)中携带安全标记的方式实现标记与数据流的绑定,并形成了 RFC1108[7]标准,相继发展的还有 CIPSO[8]、CALIPSO[9]等;其后,陆续提出 FIPS188[10]和 labeld IPSec"label-aware SADB design"草案[11]等,各自提出了支持多级安全网络的安全标记,但都采用了 IPSO 携带安全标记的方法。尽管目前常用的 IPSO 可以实现数据流携带安全标记,但是该方法存在以下不足:

a)该方法基于通信协议的格式内容,数据包加密时标记的提取不够灵活,不能实现随时随地的数据流控制,适用环境受限。

b)IPSO 等方式携带的安全标记是以人眼可感知的方式存在于数据包中的,是显式绑定方法。对于在开放网络环境中传输的数据包来说,这种攻击者可见的安全标记暴露了数据流的敏感级别,容易引起攻击者兴趣,引发针对性攻击。

为了隐蔽敏感数据流的安全标记信息,防止敏感信息流被识别,实现安全标记与数据流的隐式绑定显得尤为重要。为此,本文提出了基于包延时的安全标记与数据流隐式绑定方法 PDBLB(packet delay based label binding),引入独立于数据包内容的包延迟时间作为安全标记的载体,通过调制数据包对之间的到达间隔时延来嵌入安全标记信息。该方法为数据流安全标记提供了隐蔽性保护,并适用于数据包加密情况,能支持随时随地的数据流访问控制。提出的 PDBLB 绑定方法具有健壮性和隐蔽性,能够支持基于数据流的安全保护策略。

1 PDBLB 安全标记绑定思路

为了实现安全标记绑定的隐蔽性,则不能使用传统的在数

收稿日期: 2013-05-15; **修回日期**: 2013-06-21 **基金项目**: 国家"973"重点基础研究发展计划基金项目(2011CB311801);国家"863"计划资助项目(2012AA012704)

作者简介:冯瑜(1989-),女,福建福州人,硕士研究生,主要研究方向为网络安全(fy64356@163.com);杜学绘(1968-),女,教授,博士,主要研究方向为信息安全;曹利峰(1981-),男,讲师,博士,主要研究方向为网络安全.

据包中以显式安全标记字段的形式来实现标记与数据流的绑定,因此本文引入一个完全独立于数据包内容的安全标记载体——包延迟时间。由于数据包在网络传输过程中将产生数据包延迟(包括传输媒介时延和设备处理时延等),可以利用包延迟这种自然现象隐藏特定的信息,因此,本文提出基于包延迟时间的安全标记绑定方法 PDBLB。PDBLB 利用包延时技术,以数据包的到达间隔时延(inter-packet delay,IPD)为载体,根据安全标记信息内容调制 IPD 值,将安全标记嵌入到数据流时间特征中,实现安全标记与数据流的隐式绑定。PDBLB 安全标记与数据流绑定思想如图 1 所示。

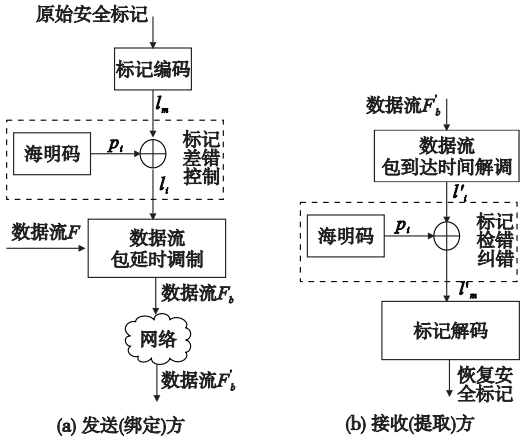


图1 PDBLB基本模型

基于包延时的数据流安全标记绑定包括发送方与接收方。发送方标记绑定模块实现安全标记与数据流的绑定(label binding),接收方标记提取模块实现数据流安全标记提取(label extracting)。

安全标记绑定模块由标记编码、标记差错控制和数据流的包延时调制组成。首先根据安全标记包含的敏感级别进行编码;然后为编码的标记添加检错纠错码;最后根据得到的安全标记码调制发送数据流,将编码的标记信息嵌入其中,实现安全标记与数据流的绑定。

标记提取模块由数据流解调、标记校验和解码组成。首先记录数据流中数据包的到达时间,从中解调获得标记校验码信息,经过检验对接收的标记信息进行检错和纠错;最后是标记解扩过程,根据已校验的编码安全标记,解码恢复出安全标记信息。

2 PDBLB 安全标记绑定方法

为权衡安全标记绑定的健壮性、隐蔽性和容量等需求,对 PDBLB 的绑定过程采取以下具体实施手段:a)引入海明码对安全标记进行检错和纠错,保证 PDBLB 的准确率;b)提出数据包随机分组方式,将安全标记的安全性分布到数据流包含的所有数据包中;c)提出包间隔时延平均值比较的安全标记与数据流绑定规则,提高对随机时间扰乱的健壮性。

下面对 PDBLB 绑定方法的安全标记编码、标记差错控制和数据流的包延时调制过程进行介绍。

2.1 安全标记编码和差错控制

多级安全信息系统中的安全标记包含受保护对象的安全等级,通常安全等级 $L=\{U,R,C,S,TS\}$,L 是一个偏序结构 unclassified < restricted < confidential < secret < top_secret。要表示 N 个不同的敏感级别,至少需要使用的码字长度为 $\log_2 N$;但为了提高安全标记的准确率,并且有一定的灵活性和扩展性,将设定码字长度为 $m(m>\log_2 N)$,安全标记码表示为 l_m。为了使得接收方能够从受网络时间扰乱的数据流中正确提取出安全标记信息,本文在数据流安全标记绑定中引入差错控制机制,为编码后的安全标记添加海明检验码[12]以实现安全标记 l_m 的检错和纠错,得到最终与数据流绑定的安全标记码表示为 l_i。

l_i(长 L)由安全标记位与标记检验位组合而成,其中安全标记 m 位,检验位 r 位。若要检测并纠正 1 位错误,需满足 $2^r-1\geqslant k+r$;若要检测2 位错误并改正 1 位错误,则满足 $2^{r-1}\geqslant k+r$。标记码与海明校验码的组合规则为:将安全标记码字与校验码自左至右进行编码,其中编码为 2 的幂次方位均为校验位,其余为标记位,如表 1 所示。

表 1 海明码合成规则

位置	B_1	B_2	B_3	B_4	B_5	B_7	B_8	B_9	…
校验位	x	x		x			x		……
标记位			x		x	x	x		…
复合位	P_1	P_2	L_1	P_3	L_2	L_3	P_4	L_4	…

将每一标记位的编码展开成 2 的幂的和(每一项不可重复),则每一项所对应的位均为该标记位的检验位。各校验位可检验的标记位为:

P_1 位检验标记位 L_1、L_3、L_5、L_7、L_9、L_{11}…

P_2 位检验标记位 L_2、L_3、L_6、L_7、L_{10}、L_{11}…

P_3 位检验标记位 L_4、L_5、L_6、L_7、L_{12}、L_{13}…

P_4 位检验标记位 L_8、L_9、L_{10}、L_{11}、L_{12}、L_{13}…

根据所检验的标记位,按照奇偶检验规则对标记位进行异或运算确定各标记校验位的值。最后按复合位顺序组合检验位和标记位,得到可纠错的安全标记码 l_i。

在接收方对安全标记码进行检错时,按奇偶校验规则对每个校验位可检验的标记位进行检错。若各校验位的值与标记位的奇偶校验值一致,则说明传输过程中的网络时间扰乱没有造成标记误码;若不一致,则可列出每个检验位的奇偶校验方程,得到检验方程组,算出错误的码位并进行纠错,最后恢复出正确的安全标记。

2.2 基于包延时的安全标记绑定

PDBLB 在安全标记绑定的实施过程中分为编码、差错控制、调制、解调、检错纠错、解码等步骤。假设发送端要发送一条安全级别为 l 的数据流 F。在嵌入安全标记之前,数据流 F 先通过发送方的安全标记编码模块对 l 进行编码、差错控制过程,得到最终与数据流绑定的二进制序列 l_i。

2.2.1 数据包分组

流 F 是一组单独的、单向的、在两个应用(发送方和接收方)之间的数据流,由五元组唯一标志。假设数据流 F 包含 n 个数据包 $\{p_i \mid i=1,2,\cdots,n\}$,数据包的原发送时间分别为 $\{t_i \mid i=1,2,\cdots,n\}$。

在绑定标记之前,其数据包间隔时延为 $\mathrm{ipd}_i=t_{i+1}-t_i$ $(i=1,2,\cdots,n-1)$。为了提高安全标记绑定的隐蔽性和提取的有效性,本文将数据包进行分组,将标记信息的绑定分布到数据流的包间隔时延中,其分组方式如图 2 所示。在 F 中随机选择 $m=L\times 2s<\lfloor n/2\rfloor$ 个数据包对,其中 $2s$ 为 PDBLB 绑定方法的冗余度。每个数据包对中包含两个连续数据包 p_j 和 p_{j+1} $(j+1<\lfloor n/2\rfloor)$。再将这 m 个数据包对分成 L 组,每组包含 $2s$

个数据包对,$L_k(k=1,2,\cdots,2s)$ 组的第 i 个数据包对表示为 $\langle p_{k,i},p_{k,i+1}\rangle(i=1,2,\cdots,2s-1)$,对应的包间隔时延表示为 $\mathrm{ipd}_{k,i}=t_{k,i+1}-t_{k,i}(i=1,2,\cdots,2s-1)$。随机地将 L_k 组的 $2s$ 个包对分成数目相等的 A、B 两组(每组 s 个数据包对)。用 $\mathrm{ipd}_{k,A,u}$ 和 $\mathrm{ipd}_{k,B,u}(u=1,\cdots,s)$ 分别表示 L_k 中 A 组和 B 组的第 u 个数据包对的 IPD。将 L_k 中 A 组和 B 组的数据包对的 IPD 均值表示为 $\mathrm{ipd}_{k,A,\mathrm{avg}}$ 和 $\mathrm{ipd}_{k,B,\mathrm{avg}}$,定义如下:

$$\begin{cases}\mathrm{ipd}_{k,A,\mathrm{avg}}=\dfrac{1}{s}\sum\limits_{u=1}^{s}\mathrm{ipd}_{k,A,u}\\ \mathrm{ipd}_{k,B,\mathrm{avg}}=\dfrac{1}{s}\sum\limits_{u=1}^{s}\mathrm{ipd}_{k,B,u}\end{cases}\quad k=1,2,\cdots,L\tag{1}$$

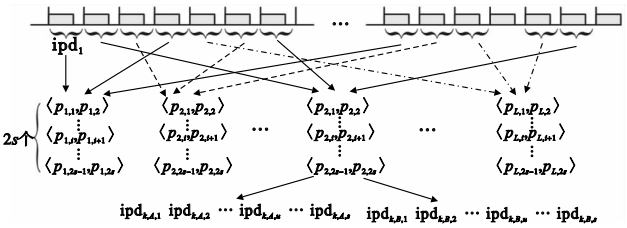


图2　数据包分组方式

2.2.2　安全标记绑定规则

在数据流中嵌入标记信息,只需调整 L_k 中 A 组和 B 组的包间隔时延平均值。若标记信息码位为 1,则使得 $\mathrm{ipd}_{k,A,\mathrm{avg}}>\mathrm{ipd}_{k,B,\mathrm{avg}}$;若标记信息为 0,则使得 $\mathrm{ipd}_{k,A,\mathrm{avg}}\leqslant\mathrm{ipd}_{k,B,\mathrm{avg}}$。

标记绑定的具体实施规则如下:

记 Δ_{ko} 为 L_k 中 A、B 组的初始 $\mathrm{ipd}_{k,A,\mathrm{avg}}$ 与 $\mathrm{ipd}_{k,B,\mathrm{avg}}$ 之间差的绝对值。

$$\Delta_{ko}=|\mathrm{ipd}_{k,A,\mathrm{avg}}-\mathrm{ipd}_{k,B,\mathrm{avg}}|\tag{2}$$

调制幅度时 a 的取值应满足 $a\geqslant\Delta_{ko}$,且其值与网络抖动处于同一数量级。使得调制完的 IPD 平均值差的绝对值:

$$\Delta_k=|\mathrm{ipd}_{k,A,\mathrm{avg}}-\mathrm{ipd}_{k,B,\mathrm{avg}}|=a\tag{3}$$

1)当标记位为 1 时

a)若 $\mathrm{ipd}_{k,A,\mathrm{avg}}>\mathrm{ipd}_{k,B,\mathrm{avg}}$,则不对数据流进行调制。

b)若 $\mathrm{ipd}_{k,A,\mathrm{avg}}=\mathrm{ipd}_{k,B,\mathrm{avg}}$,则调整 L_k 组中 A 组和 B 组的数据包的延迟时间,使其包延时均值满足 $\mathrm{ipd}_{k,A,\mathrm{avg}}>\mathrm{ipd}_{k,B,\mathrm{avg}}$。为此,将原 $\mathrm{ipd}_{k,A,\mathrm{avg}}$ 增大 a。

c)若 $\mathrm{ipd}_{k,A,\mathrm{avg}}<\mathrm{ipd}_{k,B,\mathrm{avg}}$,则调整 L_k 组中 A 组和 B 组的数据包的延时时间,使其包延时平均值满足 $\mathrm{ipd}_{k,A,\mathrm{avg}}>\mathrm{ipd}_{k,B,\mathrm{avg}}$。为此,将原 $\mathrm{ipd}_{k,A,\mathrm{avg}}$ 增大 a,同时将原 $\mathrm{ipd}_{k,B,\mathrm{avg}}$ 减小 a。

2)当标记位为 0 时

a)若 $\mathrm{ipd}_{k,A,\mathrm{avg}}>\mathrm{ipd}_{k,B,\mathrm{avg}}$,则调整 L_k 组中 A 组和 B 组的数据包的延时时间,使其包延时均值满足 $\mathrm{ipd}_{k,A,\mathrm{avg}}\leqslant\mathrm{ipd}_{k,B,\mathrm{avg}}$。为此,将原 $\mathrm{ipd}_{k,A,\mathrm{avg}}$ 减小 a,同时将原 $\mathrm{ipd}_{k,B,\mathrm{avg}}$ 增大 a。

b)若 $\mathrm{ipd}_{k,A,\mathrm{avg}}\leqslant\mathrm{ipd}_{k,B,\mathrm{avg}}$,则不对数据流进行调制。

2.2.3　数据流调制

为了实现标记位到数据流的绑定,需要对 $\mathrm{ipd}_{k,A,\mathrm{avg}}$ 和 $\mathrm{ipd}_{k,B,\mathrm{avg}}$ 进行调制。根据式(1),要在 $\mathrm{ipd}_{k,A,\mathrm{avg}}$ 上增加调制时延 a 时,只需将该组中所有数据包对的每个包间隔时延加上 a,即对每个数据包对 $\langle p_{k,i},p_{k,i+1}\rangle(i=1,2,\cdots,2s-1)$ 的第二个数据包 $t_{k,i+1}$ 增加延迟时间 a,如图 3(a)所示;若要使 $\mathrm{ipd}_{k,A,\mathrm{avg}}$ 值减小 a,则将该组中所有数据包对的每个包间隔时延减少 a,即对每个数据包对 $\langle p_{k,i},p_{k,i+1}\rangle(i=1,2,\cdots,2s-1)$ 的第一个数据包 $t_{k,i+1}$ 增加延迟时间 a,如图 3(b)所示。

3　PDBLB 安全标记提取方法

标记提取是接收方从数据流中提取恢复出发送方绑定在数据流上的安全标记信息。为了能正确解析出标记信息,接收方需要与发送方提前共享标记绑定的相关信息,如数据包随机选择函数 R、与嵌入 1 bit 标记所需数据包数量成正比的参数 s、安全标记编码方法以及海明校验码长度等。

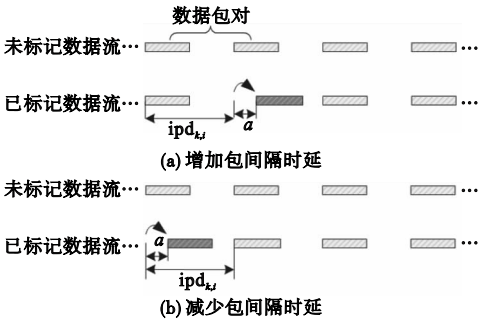


图3　包延迟时间调制

接收方的数据流安全标记提取如图 1(b)所示,包括包时间解调、编码纠错和标记解码步骤:

a)记录数据流中所有数据包的到达时间 $\{t_i\mid i=1,2,\cdots,n\}$,利用数据包随机选择函数 F 从中选择 $m=L\times 2s<\lfloor n/2\rfloor$ 个数据包对,并分成 L 个组,每组分为包含 s 个数据包对的 A、B 两组。

b)计算 A、B 组中数据包对的包间隔时延 $\mathrm{ipd}_{k,i}=t_{k,i+1}-t_{k,i}(i=1,2,\cdots,2s-1)$ 以及数据包对的 IPD 均值 $\mathrm{ipd}_{k,A,\mathrm{avg}}$ 和 $\mathrm{ipd}_{k,B,\mathrm{avg}}$。

c)根据解调规则,分别恢复出 L bit 的标记编码。对于每一位的标记编码 l_k',判决规则如下:

$$l_k'=\begin{cases}1 & \mathrm{ipd}_{k,A,\mathrm{avg}}>\mathrm{ipd}_{k,B,\mathrm{avg}}\\ 0 & \mathrm{ipd}_{k,A,\mathrm{avg}}\leqslant\mathrm{ipd}_{k,B,\mathrm{avg}}\end{cases}\tag{4}$$

d)将解调得到的 L 位的安全标记码利用海明码检错纠错规则对其进行检错纠错。

e)依据编码方式,解码获得安全标记信息。

4　安全标记健壮性理论分析

对于数据流安全标记而言,接收方能准确提取出安全标记是其基本要求,这要求安全标记具有一定的健壮性,即安全标记在随数据流传输中即使遭受网络随机时间扰乱后仍能被接收方正确识别。下面对安全标记绑定及提取的健壮性进行理论分析。

数据流 F 中任意一组 $L_k(k=1,2,\cdots,L)$,假设网络抖动给一个数据流内的每个数据包造成的时间延迟是独立同分布的,且干扰造成的数据包时延最大值为 D。组 L_k 内每对数据包 $\langle p_{k,i},p_{k,i+1}\rangle(i=1,2,\cdots,2s-1)$ 增加的延迟时间对为 $\langle d_{k,i},d_{k,i+1}\rangle(i=1,2,\cdots,2s-1)$,$L_k$ 分为 A、B 两组,网络抖动加入到各组中的随机延迟为两组随机样本 $\langle d_{A,k,i},d_{A,k,i+1}\rangle$ 和 $\langle d_{B,k,i},d_{B,k,i+1}\rangle(i=1,2,\cdots,s-1)$。令 $X_{k,A,i}=d_{k,A,i+1}-d_{k,A,i}$ 和 $X_{k,B,i}=d_{k,B,i+1}-d_{k,B,i}(i=1,2,\cdots,s-1)$ 分别表示网络对 L_k 中 A、B 组第 i 个 IPD 的干扰值,$\overline{X_{k,A}}$ 和 $\overline{X_{k,B}}$ 表示网络对 IPD 造成干扰的平均值,有

$$\overline{X_{k,A}}=\frac{1}{s}\sum_{i=1}^{s}(d_{k,A,i+1}-d_{k,A,i})=\frac{1}{s}\sum_{i=1}^{s}X_{k,A,i}\tag{5}$$

经过随机延时干扰的网络传输后,接收方在标记提取时得到的 L_k 中 A 组的包间隔时延平均值为 $\mathrm{ipd}_{k,A,\mathrm{avg}}'$,由式(1)得

$$\mathrm{ipd}_{k,A,\mathrm{avg}}'=\mathrm{ipd}_{k,A,\mathrm{avg}}+\overline{X_{k,A}}\tag{6}$$

同理有 $\mathrm{ipd}_{k,B,\mathrm{avg}}'=\mathrm{ipd}_{k,B,\mathrm{avg}}+\overline{X_{k,B}}$。因此,网络在 $\mathrm{ipd}_{k,A,\mathrm{avg}}$ 和

$ipd_{k,B,avg}$加入的随机干扰值分别为$\overline{X_{k,A}}$和$\overline{X_{k,B}}$。为了使网络随机延时不影响安全的正确提取,必须使得 $ipd_{k,A,avg}'$和 $ipd_{k,B,avg}'$与发送方的标记绑定规则一致,即保证满足以下条件:

a)当 $ipd_{k,A,avg} > ipd_{k,B,avg}$时,有 $ipd_{k,A,avg}' > ipd_{k,B,avg}'$成立,由式(3)和(6)得$\overline{X_{k,A}} - \overline{X_{k,B}} > -a$。

b)当 $ipd_{k,A,avg} \leqslant ipd_{k,B,avg}$时,有 $ipd_{k,A,avg}' \leqslant ipd_{k,B,avg}'$成立,即式(3)和(6)得$\overline{X_{k,A}} - \overline{X_{k,B}} \leqslant a$。

令 $Y_k = \overline{X_{k,A}} - \overline{X_{k,B}}$,定义正确提取 1 bit 安全标记的概率为安全标记健壮性概率 $p = Pr(|Y_k| < a)$。类似地,定义安全标记脆弱性概率 $p = Pr(|Y_k| \geqslant a)$。

假设网络抖动对数据包延迟的时间独立同分布,则随机变量 $X_{k,A,1}, X_{k,A,2}, \cdots, X_{k,A,s}$ 相互独立且服从同一分布,有 $E(X_{k,A,i}) = E(d_{k,A,i+1}) - E(d_{k,A,i}) = 0$, $\mathrm{Var}(X_{k,A,i}) = \mathrm{Var}(d_{k,A,i+1}) + \mathrm{Var}(d_{k,A,i}) = 2\sigma^2$,对随机变量 $X_{k,A,1}, X_{k,A,2}, \cdots, X_{k,A,s}$应用中心极限定理,则随机变量平均值 $\overline{X_{k,A}} = \frac{1}{s}\sum_{i=1}^{s}(d_{k,A,i+1} - d_{k,A,i}) = \frac{1}{s}\sum_{i=1}^{s}X_{k,A,i}$满足

$$Pr\left[\frac{\sqrt{s}(\overline{X_{k,A}} - E(X_i))}{\sqrt{\mathrm{Var}(X_i)}} < x\right], Pr\left[\frac{\sqrt{s}(\overline{X_{k,A}})}{\sqrt{2}\sigma} < x\right] \approx \Phi(x) \qquad (7)$$

即$\overline{X_{k,A}} \overset{近似的}{\sim} N(0, \frac{2\sigma^2}{s})$,同样有$\overline{X_{k,B}} \overset{近似的}{\sim} N(0, \frac{2\sigma^2}{s})$。这意味着网络对 $ipd_{k,A,avg}$和 $ipd_{k,B,avg}$引入的延迟服从均值为 0、方差为 $2\sigma^2/s$ 的正态分布。由此,可以得到

$$E(Y_k) = E(\overline{X_{k,A}}) - E(\overline{X_{k,B}}) = 0$$

及

$$\mathrm{Var}(Y_i) = \mathrm{Var}(\overline{X_{k,A}}) + \mathrm{Var}(\overline{X_{k,B}}) = \frac{4\sigma^2}{s}$$

则 Y_k 近似服从均值为 0、方差为 $4\sigma^2/s$ 的正态分布。

$$Pr[Y_k < x] = Pr\left[\frac{\sqrt{s}Y_k}{2\sigma} < \frac{\sqrt{s}x}{2\sigma}\right] \approx \Phi\left(\frac{\sqrt{s}x}{2\sigma}\right)$$

或

$$Pr\left[\left|\frac{\sqrt{s}Y_k}{2\sigma}\right| < \frac{\sqrt{s}x}{2\sigma}\right] \approx 2\Phi\left(\frac{\sqrt{s}x}{2\sigma}\right) - 1 \qquad (8)$$

因此,安全标记 1 bit 位的正确提取概率,即健壮性概率为

$$p_e = Pr[|Y|_k < a] \approx 2\Phi\left(\frac{\sqrt{s}a}{2\sigma}\right) - 1 \qquad (9)$$

对于长 L 位的安全标记编码,其正确提取率为 $p_L = p_e^L$。

根据式(9),对于给定调制幅度 a,安全标记正确提取率随着绑定冗余度的增大或 σ 的减小而增大,反之亦然。另一方面,要提高安全标记健壮性,必须增大$\sqrt{s}a/2\sigma$ 值,可采取的方法有增加冗余度和增大调制幅度两种。同时式(9)表明,对于网络或者攻击者引起的任意独立同分布的随机时间延迟扰乱,可以通过调节参数 s 和 a 的值来提高安全标记提取准确率,使得标记的提取准确率无限地接近 100%。

5 实验

为评估 PDBLB 的健壮性和有效性,搭建如图 4 所示的实验环境。在发送方与接收方搭建 Linux 2.6 系统,并分别安装有安全标记绑定模块和安全标记提取模块。

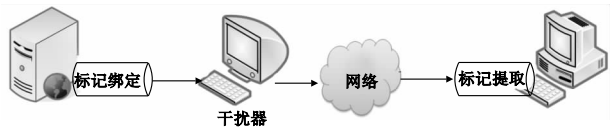


图4 实验环境设置

发送方对发出的数据流实施安全标记绑定;接收方对到达的数据流进行安全标记提取。观察接收方提取出的安全标记,计算安全标记绑定方法的准确率。每次实验使用 600 组随机数据流,每条数据流至少包含 1 000 个数据包。

PDBLB 安全标记绑定过程主要包含生成安全标记码字和基于包延时的安全标记绑定两个步骤。在准确率实验中,发送方生成安全标记码字长度为 L 位,包含 m 位校验位和 r 位安全标记位,然后根据绑定规则在包延迟时间中嵌入比特值;安全标记提取时,从数据流中提取出 L 位比特值,再根据海明码检验规则从中检测出错误并纠正。为了更清晰和直观地体现两个过程对 PDBLB 健壮性的影响,本文对两个步骤各进行实验。

实验 1 评估包延时调制绑定方法的有效性,此时不考虑海明码的纠错特性。由理论分析表明,影响包延时调制绑定方法准确率的主要因素包括调制幅度 a、冗余度 $2s$ 和安全标记编码长度。实验 1 中发送方只将 r 位安全标记码与数据流绑定,然后对各影响参数逐一测试。

实验 2 评估海明检验码对 PDBLB 健壮性的影响。该实验中,发送方将 L 位的安全标记码(包含 m 位校验位和 r 位安全标记位)与数据流绑定,在攻击者较大干扰的情况下,评估添加检验码后安全标记的准确性。

5.1 包延时调制对 PDBLB 准确率的影响

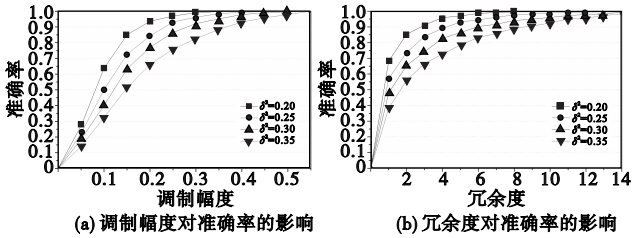
理论分析表明,影响安全标记准确率的主要因素包括调制幅度、参数 s。在实验 1 中,发送方在发送数据流中嵌入 8 bit 安全标记(如公开密级编码“0000 0000”),对两个影响因素进行逐一测试。

1)调制幅度对准确率的影响

为测试调制幅度对准确率的影响,设定冗余度 $s = 12$,分别测试不同程度的随机时间扰乱下,调制幅度对准确率的影响。实验结果如图 5(a)所示,检测度随着调制幅度的增加而增大,与分析结果一致。从图中可以看出,对不同程度的时间扰乱,只要调制幅度足够大,仍能达到近 100% 的准确率。

2)冗余度对准确率的影响

为测试冗余度对准确率的影响,设定调制幅度 $a = 0.4$,分别测试在不同程度的随机时间扰乱下,调制幅度对准确率的影响。实验结果如图 5(b)所示,检测度随着冗余度的增加而增大,与分析结果一致。从图中可以看出,对不同程度的时间扰乱,只要调制幅度足够大,仍能达到近 100% 的准确率。



(a)调制幅度对准确率的影响 (b)冗余度对准确率的影响

图5 包延时调制的准确率

由实验 1 可以看出,对网络随机时间扰乱,只要设置适当的调制速度和冗余度,就能使得接收方提取安全标记的准确率接近 100%,保证了 PDBLB 具有足够的健壮性。而面对主动时间扰乱时,攻击者引入的时延值较大,此时,准确率将随着扰乱值的增大而降低。包延时的调制方法能够保证一定的准确率,但是不能对错误比特位进行检错和纠错。通过实验 2 评估海明校验码对 PDBLB 安全标记提取的影响。

5.2 海明校验码对 PDBLB 准确率的影响

设定调制幅度 $a = 0.5$,冗余度 $s = 12$,引入主动时间扰乱。

实验检测发送方绑定只包含 8 位安全标记位信息及绑定包含 8 位标记位和 4 位检验位时的准确率,如表 2 所示。

表 2　海明码对准确率的影响

准确率	σ^2							
	0.80	0.90	1.0	1.1	1.20	1.300	1.4	1.5
8 bit 准确率/%	72.1	66.4	61.4	56.9	53.0	49.5	46.4	43.6
12 bit 准确率/%	99.9	98.5	94.7	89.3	83.3	77.4	71.8	66.7

由表 1 可以看出,当引入的主动时间扰乱较大时,若未添加检验码,则安全标记的准确率较低,且随干扰的增大而减小。当在安全标记中添加 4 bit 校验位后,虽然增加了使用的数据包数量,但安全标记的准确率得到了很大的提高。因此,在相同的时间扰乱下引入海明校验码,提高了 PDBLB 的准确率。

6　结束语

为解决 IPSO 显式安全标记绑定存在的问题,本文为数据流安全标记引入了一种与数据包内容无关的基于包延时的安全标记载体,提出了一种新的隐式安全标记与数据流绑定方法 PDBLB。在发送方的绑定过程中引入海明码实现安全标记编码的差错控制,设计了数据包随机分组方式,制定了绑定的实施规则,通过编码、差错控制、数据包分组和包延迟调制等步骤,以数据包延迟时间为载体,实现了安全标记与数据流的绑定;接收方通过延迟时间解调、纠错、解码等步骤,将安全标记信息恢复出来,完成安全标记与数据的绑定过程。PDBLB 不受数据包加密限制,具有良好的隐蔽性和灵活性;同时该方法对独立同分布的随机时间扰乱具有健壮性,保证了安全标记在随数据流传输过程中的安全性和准确性。下一步的工作将评估 PDBLB 方法的容量问题,并研究在保证安全标记绑定隐蔽性和健壮性的情况下降低绑定过程的复杂度;建立通用的安全标记与数据流绑定框架,规范绑定过程并提出适当的评估指标。

参考文献:

[1] 边力. 基于多维域特征安全标记的文件访问控制关键技术研究[D]. 郑州:解放军信息工程大学, 2012.

[2] NOBLE W B, MA ERSKI E R, VU H T. Secure data sharing system: United States, US7185066B2[P]. 2007.

[3] 王雷, 庄毅. 基于强制访问控制的文件安全监控系统的设计与实现[J]. 计算机应用,2006,26(12): 2941-2944.

[4] DONALD B, ARTHUR T, WILLIAM C. Multilevel secure database: United States, US 7539682B2[P]. 2009.

[5] TERENCE T. Multi-level and multi-category: United States, US7134022B2[P]. 2006.

[6] OUDKERK S, BRYANT I. A proposal for an XML confidentiality label and related binding of metadata to data objects, MP-IST-091-22 [R]. [S. l.]: NATO C3 Agency, 2010.

[7] KENT C. RFC 1108, Security options for the Internet protocol[S]. [S. l.]: U. S. Department of Defense, 1991.

[8] IETF CIPSO Working Group. Common IP security option version 2.3 [EB/OL]. (1993-03)[2012]. http://tools. ietf. org/pdf/draft-ietf-cipso-ipsecurity-01. pdf.

[9] STJOHNS M. RFC 5570, Common architecture label IPv6 security option(CAL IPSO)[S]. [S. l.]: U. S. Department of Defense, 2009.

[10] BROWN R H. FIPS188, Standard security label for information transfer[S]. [S. l.]: U. S. Department of Defense, 1994.

[11] BILL S. Labeled-aware SADB design[EB/OL]. (2008)[2013]. http://arc. opensolaris. org/case/PSARC/2008/252/inception. materials/phase1. pdf.

[12] HAMMING R W. Error detecting and error correcting codes[J]. Bell System Technical Journal, 1950, 26(2): 147-160.

(上接第 570 页)

4　结束语

本文结合 9/7 双正交提升小波和图像的矩阵奇异值分解实现了彩色图像水印加密算法,通过计算机仿真实验证明该算法可以很好地兼顾不可感知性和鲁棒性:对于各种常见的信号处理操作,如平滑、加噪声等攻击有很强的抵抗能力;奇异值分解的引入使得算法对常见的几何操作如旋转、剪切等攻击同样具有很好的鲁棒性。彩色水印图像预处理采用了结合骑士巡游和 Arnold 的置乱算法,在保证对水印图像置乱能力的基础上加大了密钥数据量,大大提高了算法的安全性。本文实现的方法具有计算简单、精确度高、运算速度快、安全性高等优点,能很好地应用在网络环境中保护版权和信息安全等方面。

参考文献:

[1] 姜月秋,王平,高宏伟,等. 空间域彩色水印嵌入算法研究[J]. 沈阳理工大学学报,2011,30(2):64-66.

[2] 李海燕. 一种 DCT 域的彩色图像数字水印算法[J]. 合肥工业大学学报:自然科学版,2009,32(7):1034-1036.

[3] 胡家生. 变换域数字图像技术[D]. 西安:西安交通大学,2006.

[4] 韩绍程,罗长杰,张兆宁. 基于多小波变换和分块 SVD 的彩色图像水印算法[J]. 工程图学学报,2010,2(2): 128-133.

[5] 安虎,李怡璇,徐力,等. 基于曲波变换的彩色图像零水印研究[J]. 电子测量技术,2010,33(2):45-48.

[6] 成利敏. 基于小波变换的彩色图像数字水印系统研究[D]. 天津:河北工业大学,2007.

[7] 刘志军. 基于小波域的自适应盲检彩色水印算法[J]. 计算机应用,2008,28(7):1792-1794.

[8] 薛俊玲. 基于小波变换的鲁棒性水印研究[D]. 南京:南京理工大学,2009.

[9] DOGAN S, TUNCER T, AVCI E, *et al*. A new watermarking system based on discrete cosine transform (DCT) in color biometric images [J]. Journal of Medical Systems, 2011, 36 (4): 2379-2385.

[10] MILIND E , MUNAGA V N K P, ASHUTOSH S. Singular value decomposition (SVD) based attack on different watermarking schemes [J]. Computing Letters, 2006, 2(3): 149-154.

[11] CHEN Yong-chang, YU Wei-yu, FENG Jiu-chao. A digital watermarking based on discrete fractional Fourier transformation DWT and SVD [C]//Proc of the 24th Chinese Control and Decision Conference. Shenyang: Northeastern University Press, 2012: 1383-1386.

[12] LIU Lian-shan, LI Ren-hou, GAO Qi. DWT-based robust color image watermarking scheme[J]. Journal of Southwest Jiaotong University, 2005, 13(2): 130-134.

[13] 桂国富,蒋铃鸽. 采用小波变换方法的彩色图像水印方案[J]. 哈尔滨工业大学学报,2008,40(11):1805-1807.