文章编号:1671-8836(2013)02-0171-07

高隐蔽性的无线网络主动钓鱼攻击及其防范研究

陈 伟[1,2],顾 杨[1],于 乐[1]
(1.南京邮电大学 计算机学院,江苏 南京 210023;
2.江苏省无线传感网高技术研究重点实验室,江苏 南京 210003)

摘 要:提出一种新的无线网络钓鱼攻击,该攻击采用主动攻击方式,将受害者切换到钓鱼无线接入点,同时使用低速率无线网络攻击以提高隐蔽性,并讨论了高隐蔽性无线主动钓鱼攻击模型和攻击条件,给出了一种实现此攻击的具体方法以证明其可行性.同时,针对该类型攻击提出了一种基于累加和控制(CUSUM)的检测方法,并验证了其有效性.

关 键 词:无线网络安全;钓鱼攻击;主动攻击;变化点检测
中图分类号:TP 393 **文献标识码**:A

A Stealthy Wireless Active Phishing Attack and Countermeasure

CHEN Wei[1,2], GU Yang[1], YU Le[1]
(1. School of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, Jiangsu, China;
2. Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, Jiangsu, China)

Abstract: This paper proposes a novel wireless phishing attack which uses active methods to switch victim to rogue phishing wireless access points. This attack utilizes stealthy row-rate wireless jamming attack to hide itself. This paper discusses the attacking model and the conditions of this stealthy active attack. A detailed method is given to show the feasibility of this attack. To defense against this attack, we propose a cumulative sum(CUSUM)-based detection method. The simulation results show that our method can efficiently detect this wireless phishing attack.

Key words: wireless network security; phishing attack; active attack; change point detection

0 引 言

许多酒店、商场、学校等公共场所部署了无线局域网,人们可以方便地使用笔记本电脑或智能手机访问互联网.然而,无线网络带来安全便利的同时,也带来了安全问题.其中,无线钓鱼攻击是指攻击者在公共场合架设一个伪装的无线接入点(AP:access point),设置与真实 AP 完全相同的名称(SSID:service set identifier),使得受害者误连上冒牌的无线接入点,进而可以窃取密码或隐私信息[1～3].目前,人们所关注的无线钓鱼攻击都属于被动攻击,即攻击者设置好钓鱼 AP 后,需要被动等待受害者.因此,这种被动钓鱼的攻击效果有限.通常真 AP 的信号强度好,离用户距离近,用户计算机的操作系统会默认连接真实的 AP.

本文提出一种新型的主动无线钓鱼攻击方式,即在设置好伪装 AP 后,攻击者可以使用主动的阻塞攻击来切断受害者与真实 AP 的连接,使受害者被迫选择连接伪装的钓鱼 AP.目前大部分的操作系统,如个人电脑上的 Windows,智能手机 Android, Windows Mobile 等,都不区分同名 AP(SSID 相同),认为是"瘦"AP 模式,即使用多个同名无线网桥建立网络连接.当某一无线 AP 出现信号不好、数据丢包等情况,操作系统会自动切换到另

收稿日期:2012-07-22
基金项目:国家重点基础研究发展计划(973)项目(2011CB302903);国家自然科学基金(61202353,61272084);江苏高校优势学科建设工程(YX002001)资助项目
作者简介:陈 伟,男,副教授,博士,现从事网络安全研究. E-mail:chenwei@njupt.edu.cn

一同名AP而不会给用户任何提示.攻击者正是利用这一特点,进行主动钓鱼攻击.这种方法可以极大地提高攻击效果,使攻击者获取其感兴趣的信息.

为破坏真实AP的网络性能,将受害者吸引到钓鱼AP上,需要使用无线阻塞攻击.此类攻击使用暴力攻击的方式,该方式如果想完全拥塞一个信道需要以很高的频率发送数据包.例如,如果一个攻击源试图使用SIFS拥塞攻击完全拥塞一个信道,它通常需要每秒钟发送50 000个数据包[4].这种攻击方式特征较为明显,可以有多种方法来检测与防范无线DoS攻击.

为了避免被发现,攻击者可能使用更加隐蔽的攻击手段.这种高隐蔽性的攻击不再使用大流量的暴力攻击数据,而是使用低速率的攻击流降低真实AP的网络性能,迫使受害者转向伪装AP[5].此类低速率的攻击以最小的代价降低网络的性能,难以被常规方法所检测.

本文将讨论高隐蔽性的无线主动钓鱼攻击及防范方法.其攻击原理是利用特定的低速率无线阻塞攻击方法,使得TCP协议传输层错误的认为这些数据包的丢失是由于网络存在拥塞,并进入一种毫无必要的重传状态,结果会导致TCP性能严重下降.这种攻击并不像暴力攻击需要连续的阻塞无线网络接口层,它只要能在特定时刻发送阻塞数据包,具有较高隐蔽性.本文所做的主要工作有:① 提出主动的无线钓鱼攻击方法,这与目前已有的被动无线钓鱼攻击有本质区别,该方法能极大增加无线钓鱼攻击的成功率.② 讨论高隐蔽性的无线主动攻击模型和攻击条件.近年来有不少研究是关于降低服务质量和低速率拒绝服务攻击的研究,但它们主要是针对有线网络[6~10].③ 提出了一个基于CUSUM的轻量级检测方法.当短时间内出现来自同一源地址的攻击数据时,流量序列的分布规律会出现一个变化点,基于CUSUM的检测方法可以根据这些变化点发出报警.

1 相关工作

在相关的研究工作中,伪装AP英文为Rogue AP,有时也称为Evil Twin AP.Ma等人[11]提出了一种检测伪装AP的保护框架,通过被动监听发现一些异常数据,对操作系统和无线网卡网络接口提取指纹,从而发现一些异常的AP.Watkins等人[12]根据数据包的往返时间(RTT:round trip time)来判断AP的真实性,可以区分有线网络节点,真实AP和伪装AP.Han等人所在的课题组针对伪装AP问题,提出了一种基于时间的检测方法[3,13],与Watkins的方法有异曲同工之处,该方法根据DNS服务器与用户之间的往返时间(RTT)来判定AP是真实的还是伪装的.在文献[1]中设定伪装AP使用原AP将数据转发回去,因此TTL跳数会增加,同时延时会有所延长,该文详细讨论了网络性能在伪装AP与原AP的区别,并以此作为检测标准.在这些方法中,如果伪装AP不通过原AP返回数据,而是使用其他互联网出口,如3G网络,这些方法的检测效果会受到影响.

Wei等人[14]根据无线网络CSMA/CA机制的特点,使用TCP ACK包对来802.11数据包头进行监控,可以有效区别以太网数据包和无线网络数据包,可进一步发现非法AP和无线网络性能下降.Song[1]的文章里面提及了伪装AP的问题,该伪装AP可以偷取密码,该文提出了基于用户端的检测方法,不需要知道AP的信息,提出了TMM(trained mean matching)和HDT(hop differentiating technique)检测算法,这两个算法都用到了序列概率测试技术(sequential probability ratio test).这些方法能在某些环境中用来检测无线伪装AP,这些伪装AP都是使用被动的攻击方法,而本文将探讨主动无线钓鱼攻击,与其有本质不同.

2 高隐蔽性的无线主动钓鱼攻击

无线主动钓鱼攻击的第一步是建立一个伪装AP,该步骤很容易实现,只要购买信号强的无线AP,参照真实AP的参数将其配置成伪装AP,大部分的被动钓鱼攻击到此就结束了,只需守株待兔等待受害者连接伪装AP.而主动钓鱼攻击需要进一步通过阻塞攻击破坏受害者与真实AP之间的网络连接,受害者才会选择连接更稳定的钓鱼AP.为了能隐藏自身,可以采用无线低速率攻击方式.无线低速攻击主要针对TCP协议中广泛使用的自适应机制算法,本节讨论利用TCP协议中重传超时机制的漏洞进行隐蔽攻击的可行性.

2.1 TCP重传超时机制中的漏洞

TCP使用重传超时机制(RTO:Retransmission Timeout)来保证数据包在网络上能够可靠的发送到目的地.在RTO机制中,TCP发送者按序列号顺序将数据包发送到接收者,当接收者收到这些包后按顺序发回ACK包进行确认信息.如果接收者没有按顺序收到数据包时,接收方将发回重复的ACK

包.如果发送者没有收到接收者的 ACK 包时,发送者等待一段时间,然后重新发送丢失的数据包,发送者使用超时定时器来确认数据丢失,这段超时时间被称为 RTO 定时器. RTO 值的选择直接关系到 TCP 吞吐量,可以根据网络状况通过 RTT(round-trip time)方法进行更新而达到一个比较合适的值,RFC2988 给出了计算 RTO 定时器的一个算法.

RTO 机制中存在一个漏洞,因为数据包丢失的一个标记就是发送者没有收到 ACK 包,如果攻击者故意阻止 ACK 包,发送端在等待一段时间后就会错误的认为网络存在拥塞,然后降低它的拥塞窗口重新传送. 当一个攻击者连续的阻止 ACK 包到达 TCP 发送者时,TCP 发送者将被迫重复进入重传状态,不断减小拥塞窗口,结果 TCP 吞吐量进入一种接近 0 的状态. 对于攻击者而言,不需要一直占用信道,只要在 ACK 发送的时候能准确阻塞 ACK 数据包就可以达到目的. 这种攻击相对来说平均攻击速率低,较难检测.

2.2　无线低速率攻击模型

在无线网络中,只要能成功阻止传输层的 ACK 包,就可以实现针对 TCP 的隐身攻击,一个可行的方法就是在无线网络中通过无线网络接口层阻止 ACK 包. 无线低速率攻击依赖于两个因素:第一个因素是攻击者要能成功占用信道一段时间,确保 ACK 包会因为超时被网络接口层丢弃. 第二个因素就是要重复的阻止 ACK 包,保证 TCP 发送者无法收到 ACK 包.

在第一个因素中一个重要的问题就是在何时占用信道,占用多长时间才能确保 ACK 包被丢弃. 802.11 使用竞争窗口来解决网络接口层的重传问题,当无线网络中的发送者要发送数据或者重发数据时,都有一个竞争窗口. 每一个竞争窗口分为 n 个时间片,开始 n 设为 2^5-1,如图 1 所示. 发送者从这 n 个时间片中随机选取一个时间片,并等到该时间片的到来然后试图占用信道进行发送. 如果没有得到信道,将进入重传状态等待下一次机会,这时竞争

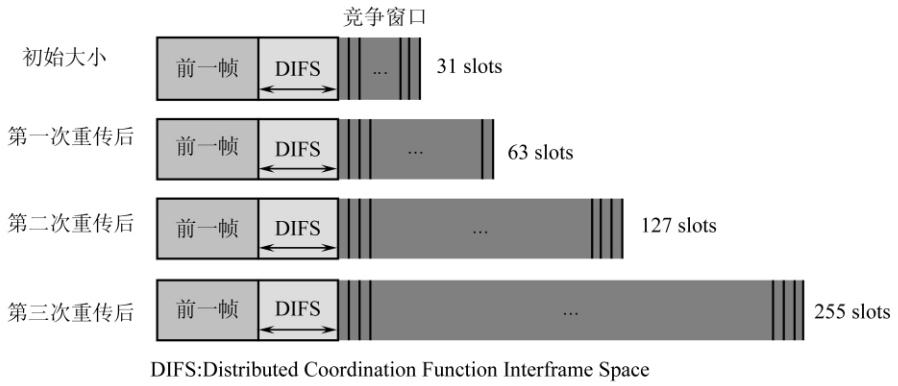

图 1　网络接口层重传后竞争窗口不断增大

窗口将增加近一倍,变为 2^6-1 个时间片,并再次从中选择一个时间片. 在 802.11 协议中最多进行 5 次重传,如果 5 次重传都失败,该包将会被丢弃.

第二个因素中要解决如何连续阻止 ACK 包的问题,这个问题可以通过研究计算 TCP 重传时间的 RTO 定时器来解决. 在特定条件下,可以使 TCP 的 RTO 值都等于 minRTO,因此需要等待的时间是 minRTO-L,L 指阻塞攻击的时间.

可以用一个带 6 个参数的模型(T,L,l_j,i,D,R)来定义隐身攻击,如图 2 所示. T 指攻击周期,L 指阻塞时间. l_j($0\leqslant j\leqslant R$)指在每一轮中阻塞攻击的时间,l_j 需要比每个拥塞窗口要大. i 是指两个相邻攻击之间的间隙. D 是指在阻塞攻击下 ACK 被丢弃的概率. R 是指在一个攻击周期 T 内所进行的攻击轮数. 攻击者为了阻止网络接口层成功重传数据,攻击者可以重复的占用信道,直到网络接口层放弃传送. R 应该大于等网络接口层重传次数(在802.11 协议中一般是 5 次).

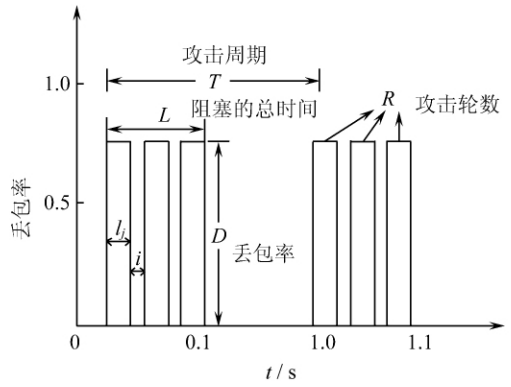

图 2　无线低速攻击的模型

可以得到无线低速攻击的条件：

1) $l \geqslant CW_j$，$0 \leqslant j < R$. 每一个阻塞时间 l 应该比网络接口层中的竞争窗口要大. CW_j 是 802.11 协议中网络接口层的竞争窗口.

2) $minRTO > SRTTi + 4 \times RTTVAR_i$，minRTO 大于 $4 \times RTTVAR_i$，RTTVAR 是 RFC2988 中定义的环回时间变量.

3) $i <$ DIFS. DIFS(Distributed coordination function interface)是指由 802.11 协议定义的分布同等函数接口.

第1个条件通过上文对第一个因素的分析容易理解. 第2个条件与文献中[6]描述一致，目的是使所有的 TCP 流都能同步它们的重传时间，这样攻击者就能影响到所有的 TCP 流，使得攻击效果最大化. 第3个条件是确保阻塞攻击在其他结点开始 MAC 层重传之前就进行攻击.

在攻击下所有的 TCP 流的吞吐量将会大约等于

$$\rho(T) = D^n \frac{\lceil \frac{L}{T} \rceil T - \text{minRTO}}{\lceil \frac{L}{T} \rceil T} + (1 - D^n) \quad (1)$$

minRTO 指最小 TCP 重传超时时间，在互联网上一般设为 1 s. 在(1)式中有一个假设是 TCP 聚集流将会在重传结束后使用所有的可用带宽. 当一个 ACK 包被成功阻止后，TCP 发送者将会等待直到 minRTO 定时器超时，然后进行重传. 因此 TCP 发送者在时间 $\lceil \frac{L}{T} \rceil T$ 时间内只能有 $\lceil \frac{L}{T} \rceil T$ -minRTO 的时间里可以充分利用可用带宽. 因此在攻击下的吞吐量是 $(\lceil \frac{L}{T} \rceil T - \text{minRTO}) / \lceil \frac{L}{T} \rceil T$，没有攻击的情况下是 1. 其中隐身攻击成功阻止 ACK 包的概率是 D^n.

从(1)式可以看出，如果 $L \leqslant T$，$T = \text{minRTO}$ 且 $D = 1$，那 $\rho(T) = 0$. 也就意味着 TCP 的 ACK 包在网络接口层被完全阻塞，TCP 的吞吐量降到了 0. 如果一个攻击者想更好的隐藏自己，他可以选择使用较小的 D，这样攻击流不需要很大，但仍然降低了无线网络的性能.

3 主动钓鱼攻击的检测方法

为了检测高隐蔽性的主动钓鱼攻击，本文使用一种基于 CUSUM 变化点检测[15]的方法. 本文在实现高隐蔽性攻击时利用了先前研究的 RTS/CTS 机制漏洞[16]，检测时使用一个 RTS 表来记录收到的 RTS 帧，并使用 CUSUM 方法来检测. 使用 CUSUM 的好处是计算量低，可以在最快的时间内发现攻击. 在正常的情况下，无线网络的信道是共享的，信道时间分配的分布是接近平均的. 但在攻击情况下，攻击者可能在一小段时间内(图1中的 L 时间内)连续强占信道，使得在局部出现不平均的情况，因此出现不满足预期分布的变化点，我们根据此特征来使用 CUSUM 检测.

在 CUSUM 方法中，设有观察到一个独立的随机序列 $X_1, \cdots, X_n$，对于 $1 \leqslant v \leqslant n$，假设 H_v 设定对于随机变量 $x_1, \cdots, x_{v-1}$，满足密度函数 $f_0(\cdot)$，对于随机变量 $x_v, \cdots x_n$ 满足密度函数 $f_1(\cdot)$，用 H_0 表示样本的随机同质性假设. 那么发现 H_v 不同于 H_0 的可能性是

$$\max_{0 \leqslant k \leqslant n}(S_n - S_k) = S_n - \min_{0 \leqslant k \leqslant n} S_k$$

其中：

$$S_0 \equiv 0, \quad S_k = \sum_{j=1}^{k} \ln \frac{f_1(x_j)}{f_0(x_j)}$$

CUSUM 方法有一种无参数的版本：

$$y_n = (y_{n-1} + x_n)^+, y_0 = 0$$

对应的判定规则是

$$d_N(\cdot) = d(y_n) = I(y_n > N)$$

其中 $I(\cdot)$ 是指示函数，N 是报警的阈值. d_N 是在时刻 n 时的判定，如果是“1”意味存在攻击，如果是“0”意味着没有攻击.

一般说来序列 X_n 的数学期望是 $E(X_n) = c$，我们选择一个参数 a 作为 c 的上界，也就是 $a > c$，然后定义一个新的序列，$x_n = X_n - a$，这样在正常操作情况下，它的值是一个负值，当攻击发生以后，其值会迅速增加，x_n 就会变成正值.

当一个新的 RTS 包到达时，它会根据 RTS 帧源地址分布情况计算出一个分值 $\text{score} = \log(a/i)$，i 是 RTS 包在 RTS 表中找到的具有相同源地址的 RTS 帧索引，如果 i 越小，说明该包在表中刚刚出现，很有可能是一个攻击者连续发送的攻击包，因此分值会比较大. 如果 a 越小，说明该包很长一段时间内没有出现，因此不太可能是由攻击者发出的. R_t 定义为 RTS 包 score 值按时间组成的序列. 如果在短时间内这些包来自同一个源地址，R_t 的分布规律就会出现变化. 在正常情况下 $E(R_t)$ 的期望值为 c，设置 a 为 c 的上界值，$c_t = C_t - a$ 在正常的情况下是负值，当攻击出现，连续的 RTS 会使 score 值增大，c_t 值变成正值，当 CUSUM 的值超越一个阈值 N 后，检测程序会发出隐身攻击警报.

4　结果与讨论

4.1　高隐蔽性无线主动钓鱼攻击的可行性

在真实网络环境中实现了高隐蔽性无线主动钓鱼攻击,图 3 显示了实验中的无线网络环境,其中包含真实 AP 和伪装钓鱼 AP,真实 AP 与路由器的连接带宽是 100 Mpbs,延时为 2 ms, AP 的传输带宽是 54 Mbps,伪装钓鱼 AP 使用 3G 网络作为互联网出口. 在 3 次实验中,真实 AP 放在 O 处,钓鱼 AP 分别放在 A,B,C 3 个地点,以检测钓鱼 AP 在不同的信号强度下对受害者的影响.

在主动攻击中,攻击者使用无线低速率阻塞攻击对受害者与真实AP发动攻击,这里利用802.11协议中的 RTS/CTS 漏洞,RTS 阻塞攻击通过发送特定的 RTS 帧实现,RTS 帧中的 NAV 字段被设置的足够长. 当攻击者连续发送出 RTS 数据包给接入点 AP,这个 AP 将用 CTS 应答,周围的结点收到 CTS 后将在 NAV 指示的时间内保持安静. 如果攻击者在一小段时间内连续发送 RTS 包,并设置较大的 NAV 值,其他正常结点可能无法正常发送数据包,导致一部分数据包丢失. 如果在这段时间内由传输层传递给网络接口层的 ACK 包受到影响,那该 ACK 包就会被丢弃. 按照前文所给出的条件发动攻击,可以使用少量的 RTS 攻击包误导 TCP 发送者进入的重传状态,导致网络吞吐量下降. 在具体实现 RTS 攻击的方法可以参考我们先前的工作[16]. 图 4 中展示了实验使用的钓鱼 AP 设备,还可以利用 Android 智能手机远程发动一次主动钓鱼攻击,增加了主动钓鱼攻击的方便性.

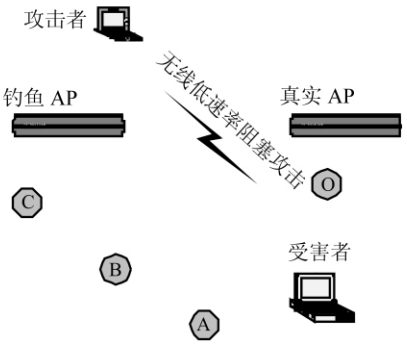

图 3　无线网络主动钓鱼攻击

当受害者被迫转到钓鱼 AP 上后,钓鱼 AP 可以将受害者的数据转发回真实 AP,或通过 3G 网络转发,所有数据将经过钓鱼 AP,可以实现中间人攻击. 由于现在针对 https 协议已经有了攻击方法,使用 https 协议的邮件系统也存在被窃取密码的可能性,如 Gmail, hotmail, yahoo, 163 等. 如果在钓鱼 AP 中使用 DNS 重定向,可以将用户引导到钓鱼网站. 所以该攻击的威胁不容轻视.

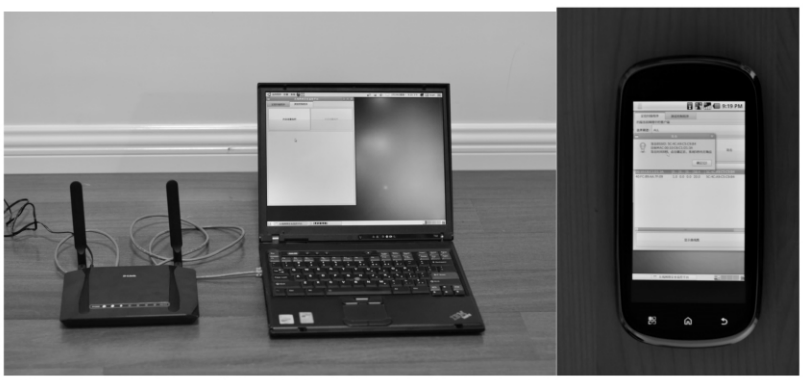

图 4　无线网络主动钓鱼攻击实验平台

实验结果显示,当采用被动攻击方式时,如果钓鱼 AP 在位置 A 时,由于信号比真实 AP 强,当受害者在第一次连接无线网络时有可能选择钓鱼 AP,但如果受害者事先已经连接到真实 AP 上,很难再选择钓鱼 AP. 如果钓鱼 AP 在位置 B 和 C 上,由于信号比真实 AP 差,被动的钓鱼方式更难以成功. 而在使用主动钓鱼方式后,无论在 A、B、C 的哪个位置,也无论受害者事先是否连接真实 AP,都可以被吸引到钓鱼 AP 上. 图 5 中显示在主动攻击成功后,钓鱼 AP 截获的 Gmail, yahoo 等采用 https 加密的邮件密码(涉及隐私,已用白框覆盖),所以别有用心的攻击者有可能可以利用主动钓鱼攻击来截取网银、第三方支付网关等敏感信息,需要引起足够的重视.

4.2　检测结果

使用同样场景来验证检测方法的效率. 实验使

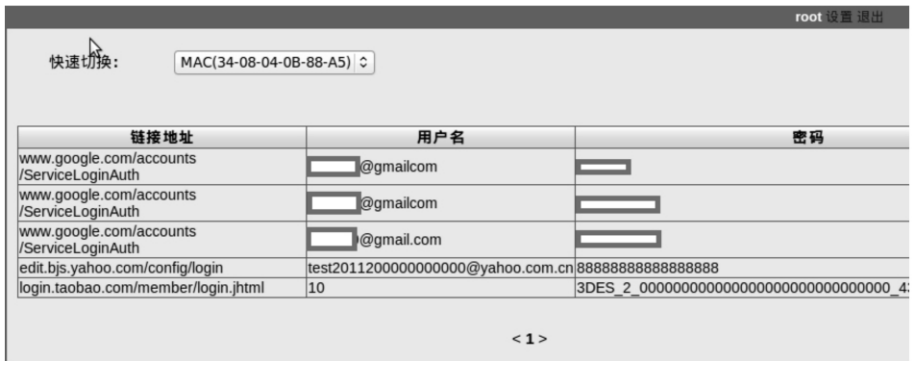

图 5 主动钓鱼攻击所截获的 https 加密信息

用两个场景来验证检测方法的效果. 一个场景中是没有主动攻击的,另一个场景中是有主动攻击的. 攻击周期 T 设为 1 s,攻击轮数 i 设为 4,RTS 表的大小设为 6,α 设为 7. 整个模拟时间为 100 s,但为了显示清晰,我们只给出了部分 CUSUM(10 s)结果.

从图 6 (b)中可以看出,当有连续的来自同一源地址的 RTS 帧被检测到之后,CUSUM 的值会显著增加,在攻击情况下可以明显的判断出攻击的存在,当 CUSUM 值超过一个阈值 N 时,检测程序将发出隐身攻击警报. 图 6 (a)显示,在正常情况下,CUSUM 的值很小,虽然有时正常用户可能会连续占用信道引发 CUSUM 值大于 0,但这种情况发生的可能性比较小,因此 CUSUM 值本身很快会恢复到 0,这样可以保证 CUSUM 方法的误警率比较低. 在实验中上界 a 根据经验设置为 1.8,阈值 N 设置为 5.

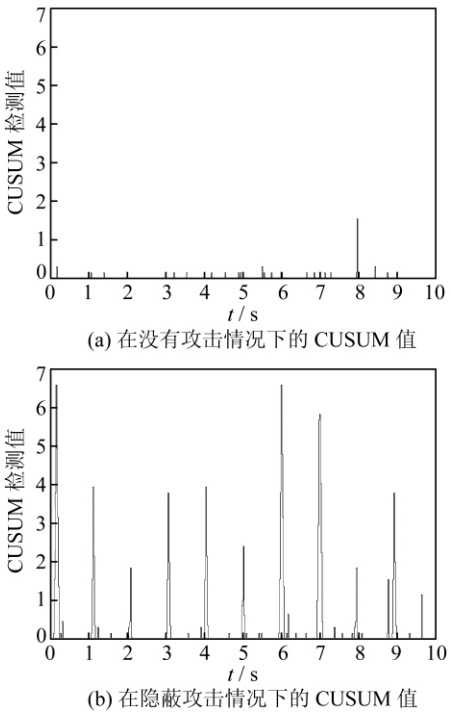

图 6 在不同场景下 CUSUM 的结果

5 结 论

本文分析了在无线局域网中发动高隐蔽性主动钓鱼攻击的可能性,提出了隐蔽式主动攻击的模型并讨论了攻击条件. 该攻击使用少量的攻击流就能严重地影响网络 TCP 吞吐量,从而主动将受害者的电脑吸引到钓鱼 AP 上. 同时由于攻击流小,很难用已有的方法检测. 针对该攻击,本文提出了一种检测该攻击的方法, NS2 模拟结果显示了隐蔽式主动攻击的效果,也验证了检测方法的有效性.

本文提出的防范方法只适用于部分主动钓鱼攻击检测,在今后的工作中我们将进一步研究较为通用的检测方法,探讨无线网络中高隐蔽性主动钓鱼攻击可能利用的漏洞,针对无线网络协议中多种自适应算法进行安全漏洞分析,提出相应的防范方法.

参考文献:

[1] Song Yimin, Yang Chao, Gu Guofei. Who is peeping at your passwords at starbucks? ——To catch an evil twin access point[C]//*Proceedings of the 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks* (*DSN'10*). Chicago, IL: IEEE Computer Society Press, 2010: 323-332.

[2] Xu F Y, Tan C C, Zhang Y F, *et al*. Defending against vehicular rogue Aps[C]//*Proceedings of IEEE 30th Annual Joint Conference of the IEEE Computer and Communications Societies* (*INFOCOM* 2011). Shanghai: IEEE Computer Society Press, 2011: 1665-1673.

[3] Sheng B, Tan C C, Li Q, *et al*. A timing-based scheme for rogue AP detection[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2011, **22**(11): 1912-1925.

[4] Bellardo J, Savage S. 802.11 denial-of-service attacks:

Real vulnerabilities and practical solutions[C]//*Proceedings of the 12th USENIX Security Symposium*. Washington DC:USENIX Association, 2003:15-28.

[5] Xu W, Trappe W, Zhang Y, *et al*. The feasibility of launching and detecting jamming attacks in wireless networks[C]//*Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing* (*MobiHoc*05). New York: ACM Press, 2005:46-57.

[6] Kuzmanovic A, Knightly E W. Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants[C]//*Proceedings of the* 2003 *Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications* (*SIGCOMM* 2003). New York:ACM Press,2003:75-86.

[7] Luo X, Chang R K C. On a new class of pulsing denial of service attacks and the defense[C]//*Proceedings of Network and Distributed System Security Symposium* 2005(*NDSS*2005). San Diego:Internet Society, 2005: 61-79.

[8] **吴志军, 张东. 低速率** DDoS **攻击的仿真和特征提取**[J]. **通信学报**, 2008,**29**(1):71-76.
Wu Zhijun, Zhang Dong. Attack simulation and signature extraction of low-rate DDoS[J]. *Journal on Communications*,2008,**29**(1):71-76(Ch).

[9] Guirguis M, Bestavros A, Matta I, *et al*. Reduction of quality (RoQ) attacks on Internet end-systems[C]//*Proceedings of IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies* (*INFOCOM* 2005). Miami: IEEE Computer Society Press,2005:1362-1372.

[10] Guirguis M, Bestavros A, Matta I. On the impact of low-rate attacks[C]//*Proceedings of the 41st IEEE International Conference on Communications* (*ICC'06*). Istanbul: IEEE Computer Society Press, 2006: 2316-2321.

[11] Ma L, Teymorian A, Cheng X. A hybrid rogue access point protection framework for commodity Wi-Fi networks[C]//*Proceedings of IEEE 27th Annual Joint Conference of the IEEE Computer and Communications Societies* (*INFOCOM* 2008). Phonix: IEEE Computer Society Press,2008:1220-1228.

[12] Watkins L, Beyah R, Corbett C. A passive approach to rogue access point detection[C]//*Proceedings of* 2007 *Global Telecommunications Conference*(*GLOBECOM* 07). Washington D C: IEEE Computer Society Press,2007:355-360.

[13] Han Hao, Sheng Bo, Tan Chiu C, *et al*. A measurement based rogue AP detection scheme[C]//*Proceedings of IEEE 28th Annual Joint Conference of the IEEE Computer and Communications Societies* (*INFOCOM* 2009). New York: IEEE Press, 2009:1593-1601.

[14] Wei W, Suh K, Wang B, *et al*. Passive online detection of 802.11 traffic using sequential hypothesis testing with TCP ACK-pairs[J]. *IEEE Transactions on Mobile Computing*,2009,**8**(3):398-412.

[15] Wang H, Zhang D L, Shin K G. Change-point monitoring for the detection of DoS attack[J]. *IEEE Transactions on Dependable and Secure Computing*, 2004,**1**(4):193-208.

[16] Chen Wei, Zhang Yingzhou, Wei Yuanchun. The feasibility of launching reduction of quality(RoQ) attacks in 802.11 wireless networks[C]//*Proceedings of 14th IEEE International Conference on Parallel and Distributed Systems* (*ICPADS'08*). Melbourne: IEEE Computer Society Press,2008:517-524.

□