



面向 WLAN 的分布式无线多步攻击模式挖掘方法研究 *

陈观林^{1,2}, 王泽兵¹, 张 泳¹

(1. 浙江大学城市学院计算机与计算科学学院 杭州 310015; 2. 浙江大学计算机学院 杭州 310027)

摘 要:入侵检测和防御技术作为网络安全防护的重要手段,在传统有线网络环境中已有较为成熟的应用。但由于无线网络的特殊性,仍很少看到 WLAN 领域无线多步攻击规划识别的研究。提出了一种融合 IEEE 802.11 协议帧主要属性进行关联分析的分布式无线多步攻击模式挖掘(DWMAPM)方法。该方法包括构造全局攻击库、建立候选攻击链、筛选候选攻击链、关联多步攻击行为和识别多步攻击模式 5 个步骤。实验结果表明,DWMAPM 方法能够适用于 WLAN 的真实攻击场景,有效挖掘出多种常见的无线多步攻击模式,可以为多步攻击意图预先识别提供基础。

关键词:多步攻击模式;无线局域网;规划识别;关联分析;网络安全

doi: 10.3969/j.issn.1000-0801.2013.11.007

Research on Distributed Wireless Multi-Step Attack Pattern Mining Method for WLAN

Chen Guanlin^{1,2}, Wang Zebing¹, Zhang Yong¹

(1.School of Computer and Computing Science, Zhejiang University City College, Hangzhou 310015, China;

2.College of Computer Science, Zhejiang University, Hangzhou 310027, China)

Abstract: As the important means of network security, intrusion detection and prevention technology have seen some preliminary applications in the traditional wired network environment. Due to the distinctive characteristics of wireless network, the applications of multi-stage attack plan recognition for WLAN are rarely seen in spite of the promising potential. A distributed wireless multi-step attack pattern mining (DWMAPM) method based on correlation analysis with the IEEE 802.11 protocol frame attributes was proposed. The method consists of five steps: constructing a global attack database, building candidate attack chains, filtering candidate attack chains, correlating multi-step attack behaviors and recognizing multi-step attack patterns. Experimental results show that DWMAPM is effective for recognizing a variety of typical attack patterns in real WLAN attack scenarios, and can provide a basis for forecasting the final attack plans.

Key words: multi-step attack pattern, WLAN, plan recognition, correlation analysis, network security

1 引言

当今世界已进入网络时代,Internet 作为全球最大的计算机互联网络,不仅极大地改善了人类的日常生活方

式,还对人类社会的政治、经济、军事和文化等方面产生了深远的影响。2013 年 7 月,中国互联网络信息中心(CNNIC)最新发布的第 32 次《中国互联网络发展状况统计报告》显示:截至 2013 年 6 月底,我国网民规模已达

* 浙江省自然科学基金资助项目(No.Y1080821),浙江省本科院校中青年学科带头人学术攀登基金资助项目(No.pd2013457)

5.91 亿人,互联网普及率为 44.1%,其中,手机网民规模达 4.64 亿人,网民中使用手机上网的人群占比提升至 78.5%^[1]。

无线局域网(wireless local area network, WLAN)的发展是近年来网民规模快速增长的一个重要原因。WLAN 具有接入速率高、网络部署快、组网灵活、架构简便等特点,不仅使得人们能够更加便捷地上网,还大大提升了用户的上网体验。但是,在 WLAN 快速发展的同时,无线网络带来的安全问题也越来越突出。美国信息安全服务公司 Trustwave 在《2012 年度全球安全报告》中统计了十大网络安全风险,其中 WLAN 相关的风险就有两个,分别是无线用户自动接入非法 AP 接入点(排名第 5)和使用 WEP 加密传输无线信息(排名第 6)^[2]。

如何保障 WLAN 安全已成为网络安全领域的一个研究热点^[3]。入侵检测和防御技术作为实现网络安全防护的重要手段,在传统有线网络环境中已有较为成熟的应用,但是由于无线网络的特殊性,将其运用到 WLAN 仍然面临着许多技术难点。如何从繁杂的无线射频信号中检测出 WLAN 非法行为,准确识别 WLAN 多步攻击所对应的攻击步骤,从而挖掘出无线多步攻击的模式,对于无线网络安全具有十分重要的意义。

本文应用云安全理论和分布式技术,综合数据挖掘与规划识别方法,对 WLAN 无线环境下的多步攻击模式挖掘展开研究,提出了一个面向 WLAN 的分布式无线多步攻击模式挖掘(distributed wireless multi-step attack pattern mining, DWMAPM)方法,能够适用于 WLAN 的真实攻击场景,可以有效挖掘出无线多步攻击模式。

2 相关研究工作

2.1 攻击规划识别概况

入侵检测和防御技术作为一种重要的网络安全技术,一直以来受到学者的广泛关注。近年来,规划识别方法作为人工智能领域的一项重要研究内容,由于其与入侵检测和防御技术有着很大的相似性,可以识别攻击者的真正意图,已在入侵检测和防御中有了尝试性的应用,并取得了一定的成果。

2001 年,Geib 和 Goldman 第一次将规划识别方法引入入侵检测领域^[4],奠定了规划识别方法在入侵检测领域应用的基础。Geib 和 Goldman 采用了基于规划执行的规划识别方法,主要解决了敌对环境中的规划识别问题^[5]。2002 年,Sheyner 等人提出了一种自动构造攻击图来识别

攻击的方法,该方法利用模型检测器自动生成攻击图,但攻击图的定义和构造具有一定的难度^[6]。同年,美国北卡罗莱纳州大学的 Ning P 及其工作组提出了一种利用攻击前后逻辑关系进行关联分析的方法,通过定义关联规则描述攻击步骤之间的前提条件和后续结果,并构造多步攻击场景,从而实现攻击规划的识别^[7]。2004 年, Ning P 等人将告警关联方法和分析工具进行了集成,专门提供了分析告警之间关联关系的 TIAA 开发包^[8]。Cuppens 等人也提出了相似的关联分析方法,利用 Prolog 谓词逻辑描述攻击行为,并根据这些攻击的前提条件和后果自动产生关联规则^[9]。IBM 公司的 Hellerstein 等人提出利用专家知识库进行攻击关联分析,从历史数据中挖掘特定的攻击模式,但定义模板过于依赖专家知识^[10]。2004 年, Qin X Z 和 Lee W K 采用一种因果网络的方法对网络攻击进行识别,该方法首先构建攻击树,并定义攻击规划库对警报集进行关联,然后将攻击树转换为因果网络,从而实现攻击规划的预测^[11]。2010 年, Wang L 和 Ghorbani A 等人提出了一种定量的警报关联度计算方法,该方法结合警报的 IP 地址信息分析攻击行为步骤间存在的关联关系,自动挖掘多步攻击模式^[12]。

2.2 无线环境中攻击规划识别的特殊性

由于 WLAN 与传统的有线网络在组网方式、攻击类型等方面都存在着较大的差异,针对 WLAN 的攻击与针对有线网络的攻击具有显著的不同,这些特殊性主要体现在以下几个方面。

- 攻击的对象不同,有线网络的攻击对象主要是明确的主机,而 WLAN 的攻击对象往往是 AP 路由器。
- 攻击的层次不同,有线网络的攻击通常针对网络层以上的层次,而 WLAN 的攻击则更为关注物理层、介质访问控制(MAC)子层等层次,因为 WLAN 攻击往往未能获取 IP 地址,只能依据 MAC 地址进行攻击。
- 攻击的手段不同,有线网络的攻击往往是探测主机的漏洞并进行入侵,而 WLAN 的攻击主要是破解无线通信的密钥,获取非法接入 WLAN 的权限。

目前典型的攻击规划识别方法大多针对有线网络环境,所检测的攻击特征往往是 IP 地址、端口号等网络层以上的数据分组特征,这对于 WLAN 环境并不适用,因为无线网络入侵检测更关注 AP 接入点等攻击对象,数据分组的检测特征更侧重 beacon 信标帧、MAC 地址和信道等网



络层以下的信息。因此,需要在 WLAN 领域进行进一步的深入研究,分析面向 WLAN 的攻击规划识别难点,研究 WLAN 中多步攻击模式挖掘方法,从而提高 WLAN 入侵的预先决策性能。

3 DWMAPM 总体框架

本文设计的 DWMAPM 方法借鉴了 Ning P 和 Cuppens 提出的基于关联分析的攻击规划识别理论,改进了 Wang L 等人提出的自动多步攻击模式发现方法,充分考虑 WLAN 环境的特点,引入 AP 信息和 IEEE 802.11 无线数据分组的属性特征,能够适用于无线多步攻击模式的识别。

DWMAPM 方法包括 5 个步骤:构造全局攻击库、建立候选攻击链、筛选候选攻击链、关联多步攻击行为和识别多步攻击模式,总体框架如图 1 所示。

分布式无线采集器为 DWMAPM 方法提供基础输入,采集器分布在 WLAN 环境中的各个不同节点,通过将无线网卡的模式设置为“监听 (monitor)”,实现基于 IEEE 802.11a/b/g 标准的无线信道侦听,捕获无线传输的所有数据分组和原始告警,然后对原始告警进行预处理,剔除无关告警和重复告警,利用攻击源的 MAC 地址、AP 的 MAC 地址等特征进行分类,将原始告警聚合为超告警 (hyper alert),为后续的多步攻击模式挖掘提供前提条件。

超告警主要考虑以下 4 个关键属性:alertType、srcMAC、dstMAC 和 timestamp,alertType 表示告警类型,srcMAC 和 dstMAC 分别表示源物理地址和目标物理地址,timestamp 表示产生告警的时间戳,在一定的时间窗口内,将超告警分为以下 3 类。

- 第 1 类超告警:将具有相同 alertType、srcMAC 和 dstMAC 属性的告警归为一类,表示同一攻击源针对同一目标持续开展的同一攻击类型。

- 第 2 类超告警:将具有相同 alertType 和 srcMAC、不同 dstMAC 属性的告警归为一类,表示同一攻击源针对不同目标开展的同一攻击类型。
- 第 3 类超告警:将具有相同 alertType 和 dstMAC、不同 srcMAC 属性的告警归为一类,表示不同攻击源针对同一目标开展的同一攻击类型。

4 DWMAPM 的具体设计

4.1 构造全局攻击库

考虑到 WLAN 环境中的多步攻击主要都是针对 AP 进行的,该步骤首先利用事先存储的所有 AP 信息,按照不同 AP 的 BSSID (即 MAC 地址) 和告警发生时间,将所有超告警转换成包含所有 AP 攻击链 (AP attack chain) 的全局攻击库 (global attack database)。

定义 1 (AP 攻击链) AP 攻击链是和同一 AP 相关的一系列有序的攻击行为序列,表示为 $AP_n(ac) = \langle at_1, \dots, at_i \rangle$, 其中, $at_i \in AT$ 攻击集合,并且每一个 at_i 的源 MAC 地址集合或者目标 MAC 地址集合中都包含了该 AP 的 MAC 地址,即 $(AP_n.MAC \in at_i.SMAC) \cup (AP_n.MAC \in at_i.DMAC)$, 同时, $AP_n(ac)$ 中的每一个攻击行为 at_i 都按时间顺序依次发生,即当 $i \leq j$ 时, $at_i.timestamp \leq at_j.timestamp$ 。

定义 2 (全局攻击库) 全局攻击库是包含了当前 WLAN 中所有 AP 的攻击链集合,表示为 $D = \{AP_1(ac), \dots, AP_n(ac)\}$, 其中, $AP_n(ac)$ 以 AP 的 MAC 地址进行排序。

将所有源 MAC 地址集合或目标 MAC 地址集合中包含该 MAC 地址的超告警按照时间顺序进行排序,就可以得到该 AP 的攻击链,为了简化,采用攻击行为的 Signature ID 值来代表某一攻击行为 at , 其中, Signature ID 用整数进行表示。如果 WLAN 中包含了 n 个 AP 路由器,将所有的 AP 攻击链按照 AP 的 MAC 地址进行排序,则可以得到全局攻击库。

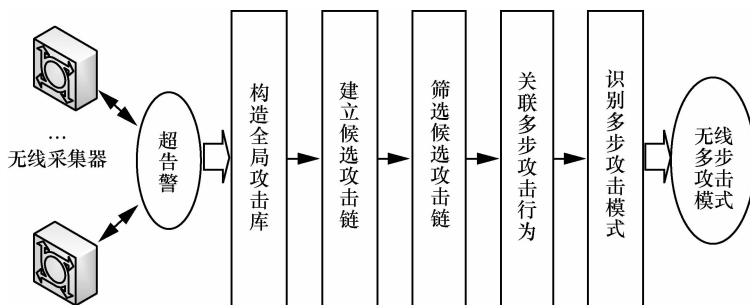


图 1 分布式无线多步攻击模式挖掘方法总体框架

4.2 建立候选攻击链

利用告警时间窗口 W_A 对全局攻击库中的所有 AP 攻击链进行划分,分别建立候选攻击链(candidate attack chain)。

定义 3 (候选攻击链) 对于全局攻击库 D 中的任一 AP 攻击链 $AP_n(ac)$, 如果该 AP 攻击链的告警时间窗口为 $W_{AP,MAC}$, 则将符合式(1)的攻击行为序列定义为候选攻击链, 表示为 AP_nAC_i 。

(1)

对于每一个 $AP_n(ac)$, 都可以利用式(1)将其划分得到多个候选攻击链, 每个候选攻击链中的所有元素都位于同一个告警时间窗口内, 需要注意的是, 这样构造的候选攻击链中的元素个数可能是不同的, 因为在相同的告警时间窗口内, 可能会产生不同数量的告警。

由于候选攻击链的建立既考虑了 AP 的告警 MAC 地址之间的关联, 又考虑了告警时间窗口的因素, 当设置一定大小的告警时间窗口时, 这样建立起来的候选攻击链中就包含了真正的无线多步攻击模式。

4.3 筛选候选攻击链

接下来需要对候选攻击链集进行筛选, 以去除这些候选攻击子链, 并删除重复的候选攻击链。

定义 4 (候选攻击子链) 对于给定的两个候选攻击链 AC_1 和 AC_2 , $AC_1 = \langle a_1, \dots, a_n \rangle$, $AC_2 = \langle b_1, \dots, b_m \rangle$, 如果 AC_2 存在下标 $i_1 < i_2 < \dots < i_n$, 使得 $a_j = b_{i_j}$ ($1 \leq j \leq n < m$), 则称 AC_1 是 AC_2 的候选攻击子链(candidate attack subchain)。

定义 5 (最长候选攻击链) 如果某一个候选攻击链 AC_i , 它不是任何其他候选攻击链的子链, 则称该候选攻击链 AC_i 为最长候选攻击链(longest candidate attack subchain)。

定义 6 (伪攻击链集合) 如果候选攻击链集合 AP_nAC 中的每一个元素都是最长候选攻击链, 且互不相同, 则称该候选攻击链集合为伪攻击链集合(pseudo attack chain set), 记为 AP_nPAC 。

筛选候选攻击链的过程也就是生成伪攻击链集合的过程, 在候选攻击链集合中去除所有的候选攻击子链, 并将重复出现的完全一样的候选攻击链删除, 最后得到其伪攻击链集合。

筛选候选攻击链的具体步骤如下。

(1) 将候选攻击链集合 AP_nAC 重新排序, 计算其中每个候选攻击链的长度, 按长度降序排列得到 $SORT(AP_nAC)$ 。

(2) 依次筛选 $SORT(AP_nAC)$ 中的每一个元素, 如果当

前候选攻击链属于其前面任何候选攻击链的子链或与之相同, 则将该候选攻击链从 $SORT(AP_nAC)$ 中删除。

(3) 重复该过程, 最后得到的 AP_nPAC 即伪攻击链集合。

4.4 关联多步攻击行为

这一步骤是整个 DWMAPM 方法的核心, 在一个实际发生的无线多步攻击场景中, 两个攻击行为之间不仅有发生时间的先后关系, 而且还存在其他属性间的关联关系。例如, 攻击者在尝试破解 AP 的 WEP 密钥前, 往往会首先对所处的 WLAN 进行探测, 在搜寻到可供攻击的具体目标后, 则会向该目标发起 deauthentication flood 攻击, 然后通过 ARP 注入进行 WEP 密钥破解。在这一完整的攻击场景中, 前后两个攻击行为的 MAC 地址和其他属性等存在着一定的关联关系。

本文提出了一个适用于 WLAN 环境的告警相关度的概念, 用量化的方式描述两个无线告警之间的关联关系, 相关度值越大, 则说明这两个无线告警属于同一个无线攻击场景的可能性越高。

定义 7 (无线告警相关度) 无线告警相关度(wireless alert correlativity) 是衡量两个无线告警之间关联关系的一个重要指标, 这两个无线告警均为无线入侵告警聚合方法输出的超告警, 对于两个先后产生的超告警 ha_i 和 ha_j , ha_i 和 ha_j 分别包含了 n 个无线属性($wa_1, \dots, wa_n$)和($wb_1, \dots, wb_n$), 则定义它们之间的无线告警相关度 $WC(ha_i, ha_j)$ 如下:

(2)

其中, w_{ij} 为不同的两个无线属性之间关联关系的权重值, 一般根据专家经验事先设置好权重值矩阵, $WAC(wa_i, wb_j)$ 为两个无线属性之间的相关度。

考虑到 WLAN 环境的特殊性, 与多步无线攻击行为相关的主要属性有以下几个: 源物理地址(srcMAC)、目标物理地址(dstMAC)、源 IP 地址(srcIP)、目标 IP 地址(dstIP) 和目标 AP 生产商(dstVendor), 因此, 选取这 5 个属性来计算无线告警相关度。

表 1 给出了这 5 个属性之间的权重值矩阵。

关于无线属性之间的权重值矩阵有如下说明。

- 为了规范计算无线告警相关度, 将权重值矩阵中所有权重值的总和设为 1。
- 由于超告警 ha_i 表示的无线攻击行为在 ha_j 表示的无线攻击行为之前发生, 因此权重值矩阵不是对称矩阵。



表 1 无线属性之间的权重值矩阵

wa_i	wa_j				
	srcMAC	dstMAC	srcIP	dstIP	dstVendor
srcMAC	0.1	0	0	0	0
dstMAC	0.1	0.25	0	0	0
srcIP	0	0	0.1	0	0
dstIP	0	0	0.1	0.15	0
dstVendor	0	0.1	0	0.1	0

- 如果权重值矩阵中的某一个权重值为 0,则表示这两个属性间不存在关联关系,权重值越大,则表示这两个属性间的关联程度越高。

4.5 识别多步攻击模式

经过上述关联多步攻击行为的步骤之后,最后通过对每一个伪攻击链中的相邻告警计算它们之间的相关度,删除那些相关度较低的攻击链,最终得到具有高相关度的攻击链,从而识别出无线多步攻击模式。

对伪攻击链集合 $AP_n.PAC$ 的每一个伪攻击链进行多步攻击模式的识别,具体识别过程如下。

(1)计算伪攻击链中每一对相邻告警之间的无线告警相关度,并与事先设置的相关度阈值进行对比。

(2)如果计算得到的相关度小于该阈值,则删除伪攻击链中这两个告警的攻击链,说明这两个告警不属于真正发生的无线多步攻击模式。

(3)如果计算得到的相关度不小于该阈值,则保留这两个告警的攻击链,因为它们很有可能属于某一个关联的无线多步攻击模式。

(4)对伪攻击链中的所有相邻告警进行以上步骤的计算之后,最后保留下来的就是识别出的无线多步攻击链,该攻击链中的每一对相邻告警都具有较高的相关度。

5 实验结果

由于目前 IDS 领域的测试数据集几乎都是基于有线网络,例如 DARPA 1998、DARPA 1999、DARPA 2000 以及 KDD CUP 1999 等都不包含 WLAN 攻击场景的数据,因此在校园网络攻防实验室内搭建了无线网络攻防实验平台,该平台包括以下 5 个部分。

- 校园 WLAN 环境,由中国移动搭建,已覆盖整个校园,无线 AP 的 SSID 统一设置为 ZUCC-CMCC,使用开放系统认证,不需要密码即可连接,建立关联

后再通过校园统一身份验证系统访问互联网。

- 网络攻防实验室自行搭建的 WLAN 环境,包括若干台设有设置加密或使用 WEP 和 WPA 加密的 AP 以及若干台配置无线网卡的台式电脑和笔记本电脑等合法终端,AP 和部分终端设备直接接入校园有线局域网。
- 无线采集器环境,包括一台配有 USB 无线网卡且安装 Snort-wireless 的台式电脑、一台配有内置无线芯片且安装 Snort-wireless 的笔记本电脑,负责采集无线网络环境中的传输数据,并输出告警。
- 模拟攻击环境,包括若干台分别安装配置 BackTrack5 和 Beini 无线攻击工具的笔记本电脑,可以实施无线探测、WEP 破解、WPA 破解、伪装欺骗、拒绝服务和会话劫持等主流的无线攻击方法。
- 控制中心环境,包括若干台控制服务器,负责无线多步攻击模式的输出等。

攻击测试和数据采集的过程如下。

(1)将无线采集器环境中两台电脑的无线网卡模式均设置为监听模式,安装配置 Snort-wireless 无线安全工具,不间断、全方位地采集无线数据分组。

(2)利用模拟攻击环境进行无线攻击测试,攻击者分别使用 BackTrack5 和 Beini 等无线网络攻击平台集成的攻击工具向校园 WLAN、实验室的两台 AP 发起攻击,攻击类型包括 war driving、DoS attack、MAC spoofing、rogue AP、evil twin 和 WEP 破解等。

(3)无线采集器捕获到和预先定义的攻击类型相匹配的数据分组,输出原始告警信息,同时将告警信息保存到控制中心的服务器中,这些原始告警信息中的绝大部分来源于模拟攻击环境,也包括少量非模拟攻击环境产生的外部告警。

在为期一周的攻击测试过程中,由于模拟攻击者实施了各类无线攻击工具对 WLAN 进行攻击,使得两个无线采集器捕获到了海量的无线数据分组,并产生了大量的原始告警信息,共计采集到原始告警 10 多万条。

利用 DWMAPM 方法进行无线多步攻击模式挖掘得到的相关结果如下。

- 对攻击测试的两个 AP 分别建立候选攻击链,此时设置告警时间窗口的值为 30 min,生成 AP_1 和 AP_2 的候选攻击链集合 $AP_1.AC$ 和 $AP_2.AC$,得到集合中的候选攻击链数分别为 21 763 条和 19 397 条。

- 对两个 AP 的候选攻击链集合 $AP_1.AC$ 和 $AP_2.AC$ 进行筛选, 删除候选攻击子链和重复的候选攻击链, 得到伪攻击链集合 $AP_1.PAC$ 和 $AP_2.PAC$, 其中的伪攻击链数分别为 627 条和 502 条。
- 对筛选后的两个 AP 的伪攻击链集合进行多步攻击行为关联, 其中, 伪攻击链中每一对相邻告警之间的无线告警相关度阈值设置为 0.5, 在对伪攻击链集合 $AP_1.PAC$ 和 $AP_2.PAC$ 进行识别的过程中, 共识别出具有高相关度的无线多步攻击模式分别为 11 组和 8 组, 这也正是利用 DWMAPM 方法挖掘出的真正发生的无线多步攻击模式。

实验结果见表 2。

表 2 DWMAPM 方法得到的相关数据结果

AP	候选攻击链数	伪攻击链数	多步攻击模式数	挖掘率
AP_1	21 763	627	11	1.75%
AP_2	19 397	502	8	1.59%

其中, 挖掘率的定义如下:

挖掘率= $\frac{\text{识别的多步攻击模式数}}{\text{伪攻击链数}} \times 100\%$ (3)

利用 DWMAPM 方法可以挖掘出多个常见的无线多步攻击模式, 如 ARP+deauthentication flood 攻击破解 WEP 密钥、wesside-ng 破解 WEP 密钥、无线路由器认证会话劫持攻击和无线路由器 config 文件窃取攻击等。

图 2 为利用 DWMAPM 方法挖掘出的针对 AP_1 的几种无线多步攻击模式, 其中, 两个相邻攻击告警之间的数值

为它们的无线告警相关度。

从图 2 中可以看出, 针对 AP_1 的每一种无线多步攻击模式中相邻攻击行为的相关度都较高, 表示实际发生的多步攻击行为之间确实存在着明显的关联关系, 特别是破解 WEP 密钥的无线多步攻击方式, 无论是 ARP + deauthentication flood 破解还是 wesside-ng 破解, 每一对相邻告警之间的无线告警相关度都在 0.6 以上, 说明这两种破解 WEP 密钥的多步攻击行为之间的关联度非常高。

利用 DWMAPM 方法挖掘出的无线多步攻击模式, 使用搭建的模拟攻击环境, 对 AP_1 实施了多种实时的无线多步攻击行为, 结果成功地预先识别出如图 2 所示的 3 种攻击行为, 这 3 种无线多步攻击方式预先识别的步数分别为 3 步、3 步和 4 步, 平均提前步数为 1.33 步, 图 3 给出了预先识别出的这 3 种无线多步攻击的预先识别步数和完整攻击步数的对比结果。

实验结果表明, DWMAPM 方法可以有效应用于 WLAN 环境, 能够自动挖掘出典型的 WLAN 多步攻击模式, 从而为多步攻击意图的实时预先识别提供基础。

6 结束语

近年来, 针对 WLAN 的入侵攻击方法不断涌现, 给个人、家庭以及公共场合部署的 WLAN 带来了严重的威胁, 保障 WLAN 的安全成为网络安全领域的研究热点。

本文提出了一种融合 IEEE 802.11 协议帧主要属性的 DWMAPM 方法, 该方法利用 AP 设备信息构造特定的全局攻击库, 引入告警时间窗口产生候选攻击链, 生成包含无线

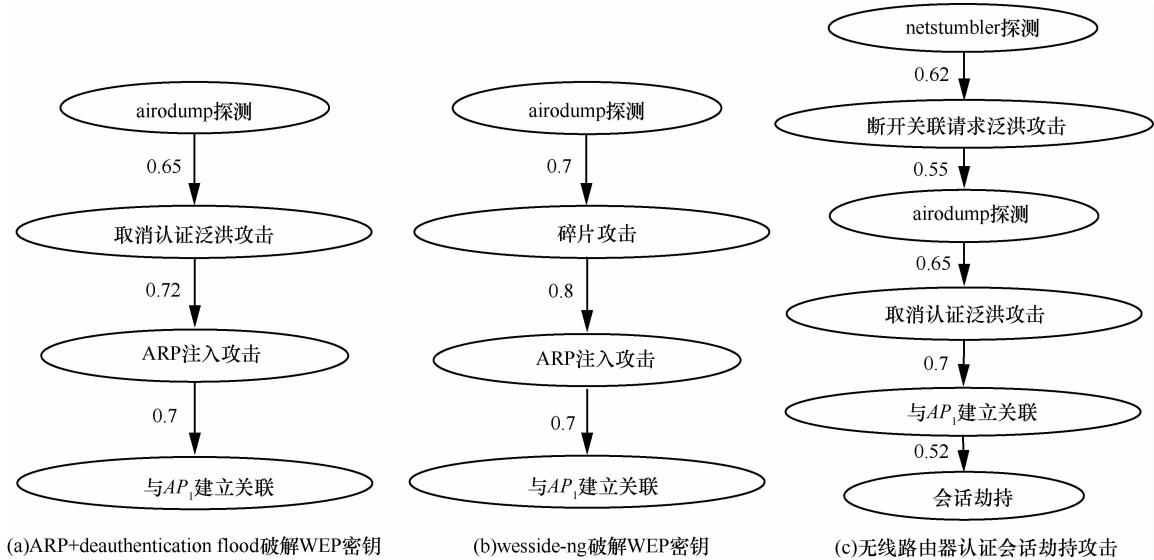


图 2 DWMAPM 方法挖掘出的无线多步攻击模式

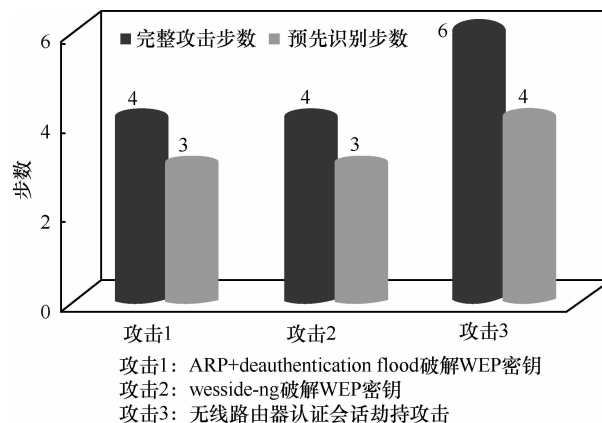


图3 预先识别步数和完整攻击步数的对比结果

多步攻击模式的伪攻击链集合,并定义了一种新的无线告警相关度的计算方法,能够自动挖掘出无线多步攻击模式。

DWMA PM方法可以识别多种无线多步攻击模式,但是需要一定的专家经验,尤其是无线告警相关度的计算需要设置合适的权重值,给无线多步攻击模式的成功挖掘带来了影响,今后将进一步研究攻击模式挖掘方法的自学习能力,减少专家的干预。

参考文献

- 1 中国互联网络信息中心 (CNNIC). 第32次中国互联网络发展状况统计报告. http://www.cnnic.cn/gywm/xwzx/rdxw/rdxx/201307/t20130717_40663.htm, 2013
- 2 Percoco N J. Trustwave 2012 Global Security Report. Chicago: Trustware SpiderLabs, 2012
- 3 陈观林,冯雁,王泽兵.分布式无线入侵防御系统预先决策引擎研究.电信科学,2010,26(10):80~86
- 4 Geib C W, Goldman R P. Plan recognition in intrusion detection systems. Proceedings of DARPA Information Survivability Conference and Exposition (DISCEX II'01), Anaheim, USA, 2001
- 5 Geib C W, Goldman R P. Probabilistic plan recognition for hostile agents. Proceedings of the Fourteenth International Florida Artificial Intelligence Research Society Conference (FLAIRS 2001), Key West, USA, 2001
- 6 Sheyner O, Haines J, Jha S, *et al.* Automated generation and analysis of attack graphs. Proceedings of the 2002 IEEE Symposium on Security and Privacy (SP'02), Oakland, USA, 2002
- 7 Ning P, Cui Y, Reeves D S. Constructing attack scenarios through correlation of intrusion alerts. Proceedings of the 9th ACM Conference on Computer and Communications Security

(CCS'02), Washington, DC, USA, 2002

- 8 Ning P, Cui Y, Reeves D S, *et al.* Techniques and tools for analyzing intrusion alerts. ACM Transactions on Information and System Security, 2004,7(2):274~318
- 9 Cuppens F, Miège A. Alert correlation in a cooperative intrusion detection framework. Proceedings of the IEEE Symposium on Security and Privacy, Oakland, California, USA, 2002
- 10 Hellerstein J L, Ma S, Perng C S. Discovering actionable patterns in event data. IBM Systems Journal, 2002,41(3):475~493
- 11 Qin X Z, Lee W K. Attack plan recognition and prediction using causal networks. Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC 2004), Tucson, USA, 2004
- 12 Wang L, Ghorbani A, Li Y. Automatic multi-step attack pattern discovering. International Journal of Network Security, 2010,10(2): 142~152

[作者简介]

陈观林,男,博士,浙江大学城市学院副教授、硕士生导师,主要研究方向为网络安全。

王泽兵,男,浙江大学城市学院教授、硕士生导师,主要研究方向为网络与数据库技术。

张泳,男,浙江大学城市学院副教授,主要研究方向为计算机应用。

(收稿日期:2013-07-30)