WLAN 中基于规范的自适应 DoS 攻击检测 *

张明雷[1], 郭渊博[1], 张来顺[1], 李雅琦[2]
(1. 解放军信息工程大学 电子技术学院, 郑州 450004; 2. 西安 68090 部队, 西安 710001)

摘 要: 无线网络由于其传输介质及通信规程的特殊性,除了要面对有线网络中存在的各种拒绝服务(denial of service, DoS)攻击之外,还面临着一些在无线环境下特有的 DoS 攻击。针对由伪造协议会话中使用的管理帧和 EAP 帧发起的 DoS 攻击,提出了一种基于规范的自适应检测方法(WSBA),为无线局域网所执行的安全协议建立在正常运行时的状态转移模型连同网络安全策略约束定义作为检测规范,作为检测此类 DoS 攻击的依据。给出了检测阈值的自适应调整算法,分析了算法参数设置对检测性能的影响。实验测试结果表明该方法是正确而有效的。

关键词: 无线局域网; 拒绝服务攻击; 有限状态自动机; 安全策略约束; 自适应阈值
中图分类号: TP393.08 **文献标志码**: A **文章编号**: 1001-3695(2010)08-3038-04
doi:10.3969/j.issn.1001-3695.2010.08.060

Specification based on adaptive DoS attacks detection in WLAN

ZHANG Ming-lei[1], GUO Yuan-bo[1], ZHANG Lai-shun[1], LI Ya-qi[2]
(1. *Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou* 450004, *China*; 2. *Xi'an* 68090 *Army, Xi'an* 710001, *China*)

Abstract: Due to the specialty of the transport medium and correspond network protocol, wireless networks not only suffer from all kinds of denial of service attacks exist in wired LAN, but also face some special DoS attacks that could only occur in wireless environment. This paper focused on those DoS attacks that launched by using fabricated management and EAP frames in WLAN. Proposed a specification based on adaptive DoS attacks detection method, built a transition model for the security protocol which wireless LAN implemented, and defined this transition model and network security policy constrains as the specification to detect DoS attacks. Also proposed an adaptive threshold adjustment algorithm and analyzed the influence of algorithm parameters to the detection performance. The result of the experiments show that the method is correct and effective.
Key words: wireless local area network; DoS attacks; finite state machine; security policy constrains; adaptive threshold

0 引言

早期的 IEEE 802.11 无线网络中存在着多种安全缺陷。IEEE 委员会提出的 802.11i 标准解决了诸多存在于 MAC 层的安全漏洞。802.11i 引入了健壮安全网络 RSNA(robust security network)的概念,RSNA 允许双向认证,引入了密钥管理协议和新的加密及完整性算法,并利用 802.1x 和 EAP 作为访问控制和认证策略[1]。

然而即使是由 802.11i 保护的无线局域网同样存在着许多的安全问题,如在 802.11i 标准中允许 RSNA 与 pre-RSNA 共存,这意味着一个 STA(station,无线客户端)可以与一个 RSNA 网络相连,也可以与一个 pre-RSNA 网络相连。在这种情况下,攻击者可能伪造一个 RSNA 配置的 AP(access point,无线接入点)的管理帧,从而发起一个针对 STA 的安全回转攻击,使 STA 配置为 pre-RSNA 模式。由于 pre-RSNA 模式采用的加密和认证算法已被证明存在着严重缺陷,攻击者可以通过这种方式攻破无线局域网。并且由于无线局域网工作在开放的传输介质上,使其容易遭受多种攻击,DoS 攻击就是其中较为严重的一种。

在 WLAN 中,攻击者可以发起多种形式的 DoS 攻击,例如攻击者可以在物理层通过广播大量的射频干扰信号,使无线信道一直处于忙碌状态,导致合法用户无法使用信道进行正常通信;由于无论是在原有的无线安全协议还是新提出的 802.11i 中都没有提出对管理帧的任何策略来保护其安全性,除了管理帧,802.11i 网络中使用的 EAP(extended authentication protocol,可扩展认证协议)帧也没有任何保护策略,攻击者可以在 MAC 层通过伪造协议交互过程中使用的管理帧和 EAP 帧等导致协议执行时出现异常,阻止协议的正常运行,从而达到拒绝服务的目的;攻击者也可以利用无线网卡驱动程序的设计缺陷,直接对用户使用的无线网卡进行攻击。这种攻击不但能够造成无线网卡程序自身崩溃,也可能导致操作系统死机或正常服务终止[2]。WLAN 中的 DoS 攻击发起手段多样,实施代价小,对网络的安全性与可用性构成了严重的威胁。

基于规范的入侵检测是由 Ko 等人[3]首先提出的,这一检

收稿日期: 2010-02-08; **修回日期**: 2010-04-01 **基金项目**: 国家"863"计划资助项目(2007AA01Z405); 国家部委预研基金资助项目(4050102020302)

作者简介: 张明雷(1986-),男,硕士研究生,主要研究方向为无线网络安全(zml19860701@126.com); 郭渊博(1975-),男,副教授,博士后,主要研究方向为容忍入侵、无线网络安全; 张来顺(1963-),男,教授,主要研究方向为网络安全、数据库安全、信息管理系统; 李雅琦(1983-),女,硕士研究生,主要研究方向为网络安全.

测技术需要定义程序的正常行为(关于某一个选定的安全协议)作为规范,随后对程序执行时违背规范的行为进行监测。Song 等人[4]利用基于规范的方法来检测无线 Ad hoc 网络中针对路由协议的攻击。其中正常行为的规范是从一个路由协议的有限状态机得到的。基于规范的入侵检测技术目前已经在多种网络环境下得到了广泛的应用,这种检测技术结合了基于特征与基于误用两种检测技术的优点,具有很好的检测效果。

本文针对 WLAN 中基于伪造管理帧和 EAP 帧发起的拒绝服务攻击,提出了一种基于规范的自适应检测方法(specification based adaptive DoS attacks detection, WSBA),对无线局域网中安全协议执行时的正常运行过程建立状态转移自动机连同网络安全策略约束定义作为检测规范,作为此类 DoS 攻击检测的依据。因为这类 DoS 攻击发生时会触发状态转移自动机的非正常转移,统计这种非正常转移的次数与预定义的阈值进行比较,若超出阈值则视为攻击。同时为了使检测方法能够更好地适应无线网络环境下的 DoS 攻击检测,本文提出了检测阈值的自适应调整算法,综合考虑无线网络环境和网络流量等信息来自动调整检测阈值,具有很强的自适应性与可扩展性。

1　相关工作

针对 WLAN 中的 DoS 攻击目前已经出现了多种检测方法:Guo[5]提出对 MAC 帧序列号进行监测,如果序列号有较大幅度的变化则表示存在攻击;Gill 等人[6]提出验证 MAC 地址是否是合法的 MAC 地址或者是合法的无线网卡提供商,或者两者的结合。但是这两种方法有效的前提是攻击者不能够伪造帧序列号与 MAC 地址,但由于 MAC 地址和帧序列号可以通过多种方式修改,攻击者可以很容易地躲避这些检测方法。Sheng 等人[7,8]提出基于物理特征监测的检测技术,一般应用以下两个参数作为检测的依据:a)信号强度(RSS),它提供了对一个接收到的信号强度的数字化的度量;b)帧往返时间(RTT)。借于无线环境的动态特征,利用物理层的参数作为检测的依据是比较难以伪造的,但是应用这些参数来检测 DoS 攻击,需要对部署的环境作出相当精细的调整,以选定合适的参数阈值来减小误报率和漏报率。

目前一些 Linux 下的开源无线入侵检测系统如 snort-wireless[9]和 WIDZ[10]同样具有对 DoS 攻击的检测能力,但是这些入侵检测系统只能够检测认证泛洪,解除认证泛洪等极少数的 DoS 攻击,检测阈值凭经验设定,检测性能对检测阈值的依赖性很强。

与上述工作不同的是,本文方法不需要限定攻击者发起攻击的条件,如不需要假设攻击者不能伪造帧序列号与 MAC 地址;另外,将网络安全策略约束加入到检测规范中,能够准确地检测只违背安全策略却遵守状态转移自动机的攻击,而且本方法针对无线环境的特点,提出了阈值的自适应调整算法,可以根据网络环境及流量动态设定检测阈值,增强了方法对网络流量状况的自适应性。

2　WSBA——基于规范的自适应 DoS 攻击检测方法

基于伪造而管理帧和 EAP 帧发起的 DoS 攻击会导致无线局域网所执行的安全协议在运行过程中出现异常。为了检测出这种异常并准确地判断出导致这种异常的原因,在本文方法中首先要建立起协议的正常运行过程。这需要将无线局域网所应用的安全协议分为多个不同的状态,建立起安全协议正常执行时的状态转移模型作为检测规范,以判断协议执行过程中是否存在 DoS 攻击。对于前面提到的安全回转攻击,由于它在不违反状态转移模型的情况下依然会导致无线局域网所执行的安全协议失效,在实现时需要对规范进行扩展,将网络安全策略约束也加入到规范中,以作为检测这类攻击的依据。

2.1　规范的构造

本文构造的规范主要由两部分组成:

a)状态转移模型。该模型的构造主要基于自动机理论,利用有限状态自动机表示无线网络安全协议的运行规则,对每一个 STA 与 AP 都建立一个有限状态自动机来表示两者建立连接的过程。协议的每一步执行都对应着自动机的相应状态转移。

有限状态自动机定义为一个五元组:

$$M=(Q,\Sigma,\delta,q_0,F)$$

其中:Q 是内部状态的有限集合;Σ 是输入字母表;δ 是状态转移函数;$q_0\in Q$ 是初态;$F\subseteq Q$ 是终态集合。

为了检测攻击者在协议运行过程中的任意时刻发起的 DoS 攻击,就必须尽量全面地描绘出协议运行过程中的正常状态转移,建立起协议正常运行时的状态转移模型作为检测 DoS 攻击的参照标准。本文以执行 802.11i 协议时 STA 的状态变迁情况为例,构造的状态转移如图 1 所示。

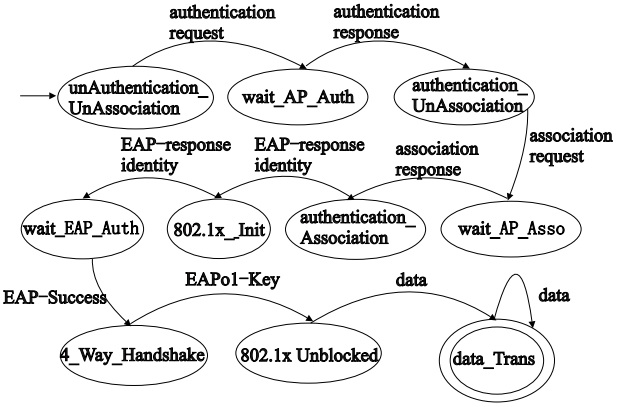

图1　执行802.11i协议时STA端的状态转移图

图 1 所对应的自动机 $M=$ ({UnAuthentication_UnAssociation, wait_AP_Auth, authentication_UnAssociation, wait_EAP_Auth, 802.1x_Init, authentication_Association, wait_AP_Asso, 4_Way_Handshake, 802.1x Unblocked, data_Trans}, {authentication request, authentication response, association request, association response, EAP-Request identity, EAP-Response identity, EAP-Success, EAPol-Key, data}, δ, UnAuthentication_UnAssociation, {data_Trans})。

定义 UnAuthentication_UnAssociation 为状态 0,wait_AP_Auth 为状态 1,依此类推,data_Trans 为状态 9。

图 1 描述了期望的 STA 状态转移,正常情况下的 STA 应严格地遵循图 1 中的顺序进行转移,即从状态 0 转移到状态 9 以建立与 AP 的安全关联。STA 只允许多次进入状态 9,这个状态是安全关联建立之后 STA 与 AP 之间可以传输数据的开始状态。其他情况下期望的状态转移应该是顺序递增的,并且

STA 的下一状态应不与它的当前状态相同。在检测过程中可能出现三种异常转移：

(a)负向转移。发生时 STA 不是从状态 0 顺序地转移到状态 9，而是从原状态转移到一个较低的状态。负向转移通常意味着攻击者利用管理帧或 EAP 帧发起了一次 DoS 攻击。虽然所有的管理帧和 EAP 帧都可以用于发起 DoS 攻击，但这些帧也同样在管理 WLAN 的资源时发挥着重要作用。因此一个负向转移不一定就代表着发生一次 DoS 攻击。为了适应合法的负向转移的情况，检测节点需要使用一个计数器来记录 STA 发生负向转移的次数，每当这个 STA 发生一次负向转移时计数器的值加 1；当计数器的值超过了阈值时，检测节点将会发出报警。

(b)正向转移。发生时 STA 不是从状态 0 顺序地转移到状态 9，而是从原状态转移到一个较原状态至少大于 1 的状态上。通常一个正向转移代表着帧丢失，但是如果在正向转移发生之前就发生了一次负向转移，则代表存在着帧伪造，会话劫持，中间人攻击。会话劫持攻击通常由两部分组成：攻击者迫使合法 STA 断开与网络的连接，通常这一步由解除关联或解除认证泛洪攻击来完成，攻击将引起状态转移模型的负向转移；随后伪造受害者 STA 的 MAC 地址来与网络进行交互，这将导致状态转移模型出现一次正向转移。

在无线网络中帧丢失是非常常见的，这可能会引起一个正向转移。例如，如果检测节点没有检测到所有的网络流量，它可能会认为 STA 的状态与它的实际状态不同。为了适应帧丢失的情况，检测节点同样需要使用一个计数器来记录正向转移的次数，当计数器的值超过了阈值时，检测节点同样将会发出报警。

(c)零转移。发生时 STA 的现状态与其原状态保持一致。在状态转移模型中(图 1)，当 STA 成功地建立了安全关联后，STA 只允许多次进入一个状态即状态 9。如果一个 STA 始终处于异于状态 9 的状态，这可能代表着错误配置或者是发生了一次 DoS 泛洪攻击而导致状态不变。检测节点将同样需要使用一个计数器来对零转移进行计数，以降低误报。

b)安全策略约束。由于攻击者可以发起安全回转攻击使 STA 与 AP 运行于低安全级别的 pre-RSNA 模式，而状态转移模型却不能很好地检测这一攻击，将网络的安全策略约束加入到规范当中，作为检测如安全回转攻击这样不违反状态转移模型但却违背安全策略的入侵。这些安全策略约束体现在网络的能力信息(RSN IE)字段支持的加密算法和需要的认证方法中。

(a)RSN 模式运行。为了监测对这一安全策略的遵循与否，检测节点将检查 AP 所广播的包含在 RSN IE 中的能力信息字段，以确定所需参数是否存在。

(b)802.1x。可以利用状态转移模型来对基于端口的访问控制进行监测。一个不支持 802.1x 的网络将不会进入到状态转移模型的状态 5 和 6(图 1)，而会从状态 4 直接转移到状态 9。

(c)AES 数据链路层加密。如 RSN 所要求的，检测节点将检测 RSN IE 并检查 AES 是否是惟一运行的加密算法。

(d)EAP-TLS 认证。对于处于状态 6 的站，检测节点将检查任何去往所监测 STA 的包含 EAP 类型为 EAP-TLS 的 EAP 请求帧，以检查 STA 与认证服务器之间是否按照 EAP-TLS 的要求完成了双向认证。

对于每一个 STA，无论何时当它发生状态转移时传感器都将检查上述这些安全策略是否正确执行，任何对这些安全策略的违背将触发一个违反安全策略的警报。

检测系统由一个工作于被动模式的检测节点来监测无线频谱，并为每一个 STA 与其关联的 AP 建立了状态转移模型。检测节点配置了由协议的状态转移模型及网络安全策略约束组成的规范。检测节点对所接收到的每一个帧都要对照规范来进行检测，以判断在协议运行过程中是否存在 DoS 攻击。

2.2 自适应阈值调整算法

由于在 WLAN 中帧丢失或重传同样会导致状态转移模型出现异常转移，需要定义一个阈值来提高检测节点适应这种现象的能力。同时，为了降低网络流量波动对检测结果的影响，并使检测过程能够自动地适应不同的无线网络环境，本文提出了检测门限的自适应调整算法，以提高报警的准确率。

令 x_n 代表在第 n 个区间内网络中的帧个数，采用简单滑动平均算法对数据进行平滑处理得到一个新的序列 $\{y_n, n = N, N+1, \cdots\}$。其中：$N$ 为滑动窗口的长度。

$$y_n = \frac{1}{N}\sum_{i=n-N+1}^{n} x_i \tag{1}$$

然后利用指数加权滑动平均算法(EWMA)得到第 n 个时间区间内的帧均值 k_n，即

$$k_n = \alpha k_{n-1} + (1-\alpha) y_n; 0 < \alpha < 1 \tag{2}$$

其中：α 为 EWMA 算法的加权系数。设 $h_{\max}$ 代表允许违反状态转移的最大帧个数，当网络搭建好后，就可以根据网络带宽与系统的处理能力得出 $h_{\max}$；β 为阈值系数。通过式(3)定义检测门限 h：

$$h = h_{\max}(1 - e^{-\beta k}); 0 < \beta < 1 \tag{3}$$

利用式(3)系统可以在不同的网络环境、不同的网络流量下自动地调整检测阈值，同时也可以通过调节阈值系数 β 使 k 与 h 保持一个良好的对应关系。

2.3 检测流程

根据之前的介绍，检测节点需要有一个训练阶段来完成以下工作：

a)确定无线局域网所执行的安全协议的各关键状态，并由此建立协议正确运行时的状态转移模型。

b)全面分析网络的安全策略约束，将各安全策略约束定义为检测规范。

c)为了应对协议执行超时的情况，应对协议执行的时间进行学习。统计出协议正常执行时的平均执行时间。

d)根据所搭建好的无线局域网，确定出最大容忍阈值。

在实际检测阶段，检测节点将按照以下流程进行检测：

a)首先检测节点将根据监测到的网络信息判断是否是一个新的协议会话，如果是，将为执行该协议的 STA 建立新的状态转移自动机；否则应找到此 STA 所对应的自动机。根据当前接收到的帧和状态转移自动机的当前状态判断下一时刻 STA 的状态。对这一 STA 的状态转移过程进行监测，若发现其违反了训练阶段建立的状态转移模型，检测节点将首先根据帧中的类型和子类型字段判断出是哪一种帧引起了这种状态转移；随后将继续判断由该帧导致的这种异常状态转移是否超

出了阈值,如果超出,检测节点将视为存在,由该帧发起的 DoS 攻击并发出报警,并根据帧中的类型和子类型字段报告出具体的攻击类型。

b)如果在 a)的检测中没有发现对状态转移模型的违反或者有违反但违反次数没有超过阈值,检测节点将继续判断当前的帧是否违反了网络的安全策略约束,若违反则发出安全报警;否则进入 c)。

c)若以上的 a)b)都能够顺利完成,检测节点将计算此协议从开始运行到结束所花费的时间,依据训练阶段得到的执行完此协议平均所需的时间,判断协议的运行是否超时,若超时检测节点将发出超时报警;否则进入 d)。

d)如果以上 a)~c)都能够顺利完成,检测节点将放行当前的帧,开始下一次的检测过程。

需要说明的是,检测节点在整个检测过程中会实时地监测网络流量,并及时更新检测阈值。检测节点的工作流程如图 2 所示。

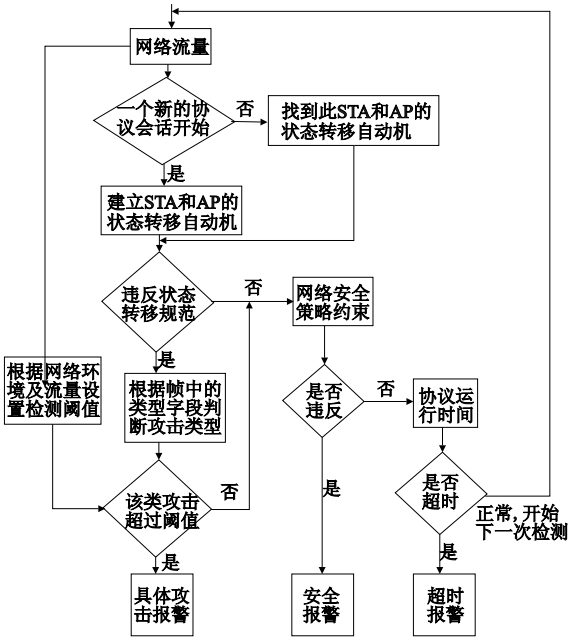

图2　检测节点的检测流程

3　实验测试

为了评估 WSBA 方法的有效性并与现有方法进行比较,本文搭建了一个测试平台,由以下几个部分构成:一个攻击节点、一个客户端节点、一个接入点、一台认证服务器及三个检测节点。三个检测节点分别执行本文所提出的 WSBA 方法、Snort-wireless 和 WIDZ。在时间段 120~210 攻击节点向 STA 与 AP 组建的连接发起了 DoS 攻击。攻击者用于发起 DoS 攻击的工具为 Back Track3 Final 版[11],这是一款可用于无线入侵的专用工具。整个测试环境的网络流量如图 3 所示,图中 x 轴代表测试时间,y 轴代表检测到的帧个数。

在测试平台搭建成功之后,根据平台的环境特征将 h_{max} 的值定义为 10。滑动窗口的长度 N 取值为 3。同时在对网络流量的监控过程中需要对阈值倍数 β 及 EWMA 参数 α 作出精细的调整,以使得报警阈值 h 可以根据网络流量的变化自动更新。由式(2)(3)可以看出,在 α 值固定的情况下,当 β 的值较大时,h 的值会接近于 h_{max},这将导致漏报的发生;而当 β 的值较小时,h 的值会随之减小,会出现较高的误报率。在进行了大量的实验之后,得出了阈值系数 β 与误警率之间的关系,如图 4 所示。

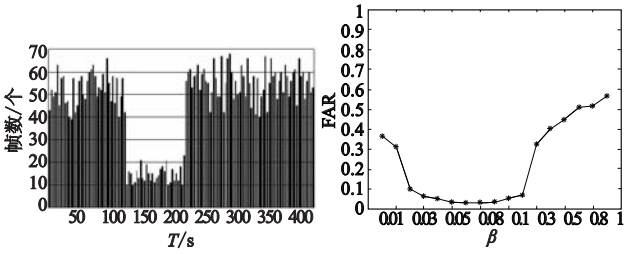

图3　测试环境的网络流量　　图4　β对误警率的影响

图 4 中 x 轴代表 β 的值,y 轴代表误警率。从图中可以看出,当 β 的值小于 0.03 或大于 0.2 时,误警率大于 10%,因此笔者建议 β 的取值为[0.03,0.2]。

在 β 的值固定的情况下,当 α 的取值增大时,则当前流量变化对流量均值的影响权重会相应地加大,h 波动较小,使得总体对流量的变化较迟钝;当 α 的取值减小时,则当前流量变化对流量均值的影响权重会相应地减少,h 波动频繁,总体对流量的变化反应较敏感。图 5(a)代表 $\alpha=0.9$ 时 h 的波动情况,(b)代表 $\alpha=0.1$ 时 h 的波动情况。通过多次实验,本文建议 α 的取值为[0.3,0.6]。

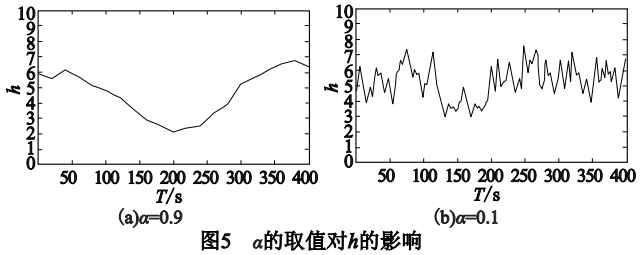

图5　α的取值对h的影响

在参数选定之后,将进入攻击的实际检测阶段,为了评估 WSBA 方法的有效性,与 Snort-wireless 和 WIDZ 等开源无线入侵检测系统在 DoS 攻击的检测效果方面进行了对比,对比结果如表 1 所示。表 1 中的"√"和"×"代表了攻击能否被成功检测。

表 1　检测结果对比

攻击	Snort-wireless	WIDZ	WSBA
解除认证泛洪攻击	√	√	√
解除关联泛洪攻击	√	√	√
认证泛洪攻击	√	√	√
关联泛洪攻击	√	√	√
EAP-Success 泛洪攻击	×	×	√
EAPol-Start 泛洪攻击	×	×	√
EAP 身份请求泛洪攻击	×	×	√
安全回转攻击	×	×	√

在对 DoS 攻击的检测效果方面,通过对比可以看出,本文提出的检测方法能够检测到实验中攻击者发起的所有 DoS 攻击,而 Snort-wireless 和 WIDZ 则只能检测到有限的几种泛洪类型攻击,并且 Snort-wireless 与 WIDZ 不具有对安全策略执行情况的监测能力。

4　结束语

本文针对 WLAN 中的 DoS 攻击提出了一种基于规范的自适应检测方法。该方法依据无线网络所执行 (下转第 3044 页)

1997,26(5):1484-1509.
[2] KITAEV A. Quantum measurements and the abelian stabilizer problem [EB/OL]. [2010-01-11]. http://arxiv.org/quant-ph/9511026.
[3] ANSHEL I, ANSHEL M, GOLDFELD D. An algebraic method for public key cryptography[J]. Math Research Letters, 1999, 6: 287-291.
[4] PAENG S H, KWON D, HA K C, *et al*. Improved public key cryptosystem using finite non-abelian groups[EB/OL]. [2010-01-11]. http://eprint.iacr.org/2001/066.
[5] ARTIN E. Theory of braids[J]. Annals of Math, 1947, 48(1): 101-126.
[6] KO K H, LEE S J, CHEON J H, *et al*. New public key cryptosystem using braid groups[C]//Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2000:166-183.
[7] ANSHEL I, ANSHEL M, FISHER B, *et al*. New key agreement protocol in braid group cryptography[C]//Lectures in Computer Science. Berlin: Springer-Verlag, 2001:1-15.
[8] CHA J C, KO K H, LEE S J, *et al*. An efficient implementation of braid groups[C]//Lecture Notes in Computer Science. London: Springer-Verlag, 2001:144-156.
[9] SIBERT H, DEHORNOY P, GIRAULT M. Entity authentication schemes using braid word reduction[EB/OL]. [2010-01-11]. http://eprint.iacr.org/2002/187.
[10] LAL S, CHATURVEDI A. Authentication schemes using braid groups [EB/OL]. [2010-01-11]. http://arXiv.org/cs.CR/0507066.
[11] 汤学明,洪帆,崔国华. 辫子群上的公钥加密算法[J]. 软件学报,2007,18(3):722-729.
[12] KO K H, CHOI D H, CHO M S, *et al*. New signature scheme using conjugacy problem[EB/OL]. [2010-01-11]. http://eprint.iacr.org/2002/168.
[13] THOMAS T, LAL A K. Group signature scheme using braid groups [EB/OL]. [2010-01-11]. http://arXiv.org/cs.CR/0602063.
[14] VERMA G K. Blind signature schemes over braid groups[EB/OL]. [2010-01-11]. http://eprint.iacr.org/2008/027.
[15] VERMA G K. A proxy signature scheme over braid groups[EB/OL]. [2010-01-11]. http://eprint.iacr.org/2008/160.
[16] ZHANG L L, ZENG J W. Proxy signature based on braid group[J]. Journal of Mathematical Study, 2008, 41(1):56-64.
[17] LAL S, VERMA V. Some proxy signature and designated verifier signature schemes over braid groups[EB/OL]. [2010-01-11]. http://arXiv.org/cs.CR/09043422.
[18] RABINM O. How to exchange secrets by oblivious transfer, Technical Report TR281[R]. [S.l.]: Aiken Computation Laboratory, Harvard University, 1981.
[19] MOROZOV K, SAVVIDES G. Computational oblivious transfer and interactive hashing[EB/OL]. [2010-01-11]. http://eprint.iacr.org/2009/074.
[20] GROHMANN B. A new protocol for 1-2 oblivious transfer [EB/OL]. [2010-01-11]. http://eprint.iacr.org/2009/172.
[21] CAMENISCH J, NEVEN G, SHELAT A. Simulatable adaptive oblivious transfer[C]//Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2007:573-590.
[22] HUANG H F, CHANG C C. A new *t*-out-*n* oblivious transfer with low bandwidth[J]. Applied Mathematical Sciences, 2007, 1(7):311-320.
[23] CACHIN C, CAMENISCH J, KILIAN J, *et al*. One-round secure computation and secure autonomous mobile agents[C]//Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2000:512-523.
[24] STADLER M, PIVETEAU J M, CAMENISCH J. Fair blind signatures[C]//Lecture Notes in Computer Science. Berlin: Springer-Verlag, 1995:209-219.
[25] JUELS A, SZYDLO M. A two-serve, sealed-bid auction protocol [C]//Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2002:72-86.
[26] 杨乐. 基于不经意传输协议的数字版权保护方案[D]. 西安:西安电子科技大学, 2008.

(上接第 3041 页)的协议及网络的安全策略约束建立起检测规范,当无线网络执行的协议发生变化时,只需将改变后的协议规范加入到检测规范当中即可,具有很强的可扩展性。同时该方法还可以根据对网络流量的在线监测自动调整检测阈值。通过仿真实验,证明了本文提出的方法在检测 DoS 攻击上的有效性。

参考文献:

[1] CHEN J C, JIANG M C, LIU Yi-wen. Wireless LAN security and IEEE 802.11i[J]. IEEE Wireless Communications, 2005, 12(1): 27-36.
[2] XING Xin-yu, SHAKSHUKI E, BENOIT D, *et al*. Security analysis and authentication improvement for IEEE 802.11i specification[C]//Proc of IEEE GLOBECOM. New Orleans, LD:[s.n], 2008:1-5.
[3] KO C, RUSCHITZKA M, LEVITT K. Execution monitoring of security critical programs in a distributed system: a specification-based approach[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 1997:175-187.
[4] SONG Tao, KO C, TSENG H T, *et al*. Formal reasoning about a specification-based intrusion detection for dynamic auto-configuration protocols in Ad hoc networks[C]//Proc of the 3rd International Workshop Formal Aspects in Security and Trust. 2005:16-33.
[5] GUO Fang-lu, CHIUEH T C. Sequence number-based MAC address spoof detection[C]//Proc of the 8th International Symposium on Recent Advances in Intrusion Detection. Berlin: Springer, 2005:309-329.
[6] GILL R, SMITH J, LOOI M, *et al*. Passive techniques for detecting session hijacking attacks in IEEE 802.11 wireless networks[C]//Proc of AusCERT. 2005:26-38.
[7] SHENG Yong, TAN K, CHEN Guan-ling, *et al*. Detecting 802.11 MAC layer spoofing using received signal strength[C]//Proc of IEEE INFOCOM. 2008:1768-1776.
[8] HSIEH W C, LO C C, LEE J C, *et al*. The implementation of a proactive wireless intrusion detection system[C]//Proc of the 4th International Conference on Computer and Information Technology. 2004: 581-586.
[9] Snort-wireless user's guide [EB/OL]. (2005). http://www.snort-wireless.org.
[10] WIDZ: the wireless intrusion detection system[EB/OL]. (2006). http://www.loud-fat-bloke.co.uk.
[11] Back track3 final[EB/OL]. (2008). http://remote-exploits.com.