



研究与开发

APT 攻击下的无线通信网络最优主动防御决策模型

孟勐, 王丹妮, 吕军, 张福良

(国网辽宁省电力有限公司信息通信分公司, 辽宁 沈阳 110006)

摘 要: 最优主动防御决策可以保障无线通信网络的安全稳定性, 为了提高无线通信网络的防御效果, 提出了 APT 攻击下的无线通信网络最优主动防御决策模型。关联无线通信网络日志, 构建 APT 攻击对象集合, 通过反馈相容系数计算 APT 攻击事件的绝对相容度, 并预测 APT 攻击行为。基于 APT 攻击源对无线通信网络攻击的信道带宽, 获取无线通信网络受到 APT 攻击的位置, 利用无线通信网络节点的权值系数, 提取无线通信网络的 APT 攻击特征。利用攻防图, 计算得到 APT 攻击对无线通信网络的损害程度, 通过定义无线通信网络的安全状态, 构建了无线通信网络最优主动防御决策模型。实验结果表明, 所提模型在防御无线通信网络的 APT 攻击时, 可以将攻击数据包拒包率和吞吐量分别提高到 90% 以上和 16 000 bit/s 以上, 并且时延较低, 具有更好的防御效果。

关键词: APT 攻击; 主动防御; 特征提取; 攻击趋势; 无线通信网络; 决策模型

中图分类号: TP393

文献标志码: A

doi: 10.11959/j.issn.1000-0801.2024020

Optimal active defense decision model of wireless communication network under APT attack

MENG Meng, WANG Danni, LYU Jun, ZHANG Fuliang

State Grid Liaoning Electric Power Supply Co., Ltd., Information & Telecommunication Branch, Shenyang 110006, China

Abstract: The optimal active defense decision can ensure the security and stability of wireless communication networks. In order to improve the defense effectiveness of wireless communication networks, an optimal active defense decision model for wireless communication networks under APT attacks was proposed. Wireless communication network logs were associated, a set of APT attack objects were constructed, the absolute compatibility of APT attack events was calculated through feedback compatibility coefficients, and APT attack behaviors were predicted. Based on the channel bandwidth of APT attack sources on wireless communication networks, the location of the wireless communication network being attacked by APT was obtained, and the weight coefficients of wireless communication network nodes were used to extract the APT attack characteristics of the wireless communication network. Using the attack and defense diagram, the degree of damage caused by APT attacks to wireless communication networks was calculated. By defining the security status of wireless communication networks, an optimal active defense decision

收稿日期: 2023-03-14; 修回日期: 2023-12-13

基金项目: 国网辽宁省电力有限公司科技项目 (No.2022YF-101)

Foundation Item: Science and Technology Project of State Grid Liaoning Electric Power Co., Ltd. (No.2022YF-101)



model for wireless communication networks was constructed. The experimental results show that the proposed model can increase the packet rejection rate and throughput of attack packets to over 90% and 16 000 bit/s respectively when defending against APT attacks in wireless communication networks, with lower time delay and better defense effectiveness.

Key words: APT attack, active defense, feature extraction, attack trend, wireless communication network, decision model

0 引言

由于无线通信网络具有结构复杂性,在网络安全防御领域,主动防御决策是非常重要的^[1]。网络安全的目标是实现从威胁到安全通信的转变,为了降低网络数据传输可能带来的安全风险,无线通信网络在安全防护方面做出了很多努力。为了应对日益复杂的通信环境,防火墙技术被应用到了更多网络中。无线通信网络在得到安全保护的同时也产生了大量问题,为了减少这些问题,需要设计一种有效的主动防御策略,从而减少系统中攻击者的攻击规模。

Huang 等^[2]提出一种轻量级系统 ScatterID,利用反向散射标签和羽毛光来减轻 Sybil 攻击的影响,通过操纵多径信号推断机器人的身份合法性。但该方法无法应对其他类型的攻击,具有一定的局限性。Chen 等^[3]提出一种最优种子调度策略算法(OSSSA)。使用连续时间马尔可夫过程对网络空间模拟防御系统模型进行数学分析,提出 OSSSA 的可靠工作机制,设计了一种可以有效评估调度算法的防御性能评估方法。但该方法忽视了实际部署中的资源限制和实时性需求,导致攻击数据包的拦截能力较低。李静轩等^[4]基于有限的网络资源,提出了最优主动防御决策研究。根据高级持续威胁(APT)攻击的意图,将非合作博弈理论应用到了网络的最优主动防御决策中,为了与 APT 攻击特征保持一致,设计一种全资产要素效用量化方法,在博弈均衡的情况下,选取了最优防御策略。但该方法无法考虑实际网络环境中的多方参与

和信息不完备的情况,影响最优防御策略的选择。王增光等^[5]以军事信息网络为研究对象,设计一种主动防御策略选取方法。根据不完全信息的博弈,对网络攻防行为进行动态建模,从网络安全角度量化处理了网络攻防行为的收益。将防御的效果和能力作为主动防御决策的选取标准,选取一种有效的主动防御方法来保护军事信息网络。但该方法在防御策略选取时,重点关注收益量化,忽视了其他重要因素。

基于以上研究背景,本文在 APT 攻击下,针对无线通信网络构建了最优主动防御决策模型,从而保证无线通信网络的安全性。

1 无线通信网络最优主动防御决策模型设计

无线信号易受电磁波干扰、物理障碍等因素影响,导致通信质量变差、数据传输中断或丢失,甚至攻击者能够更轻易地隐藏和发起攻击行为,产生更持久的影响,因此,APT 攻击在无线通信网络中更具隐蔽性和持久性。计算机网络中的主动防御并不能解决这个问题,本文通过对无线通信网络日志的关联分析,构建 APT 攻击对象集合,并利用反馈相容系数计算出 APT 攻击事件在无线通信网络中的绝对相容度,以识别和量化潜在的 APT 攻击行为。通过分析信道带宽的异常情况,发现可能存在的 APT 攻击活动。为了保护网络免受攻击的影响,增强网络的安全性和稳定性,在网络主动防御措施中,要提高对于 APT 攻击数据包的拦截和过滤,并成功拒绝这些恶意数据包的能力,即攻击数据包拒包率。简而言之,拒包率

是防御系统拒绝恶意或可疑数据包的比率,是衡量防御系统有效性的重要指标。在无线通信网络中,吞吐量是指在一定时间内通过网络传输的数据量,直接影响数据传输的速度和效率。攻击数据包吞吐量是指在单位时间内成功传输到目标系统的恶意数据包数量,用于衡量攻击的规模和强度,以及防御系统应对能力。当网络受 APT 攻击时,攻击者可能会占用网络带宽或引发其他异常行为,导致网络的吞吐量下降。本文利用权值系数考虑了节点的角色、功能和重要性,帮助识别与 APT 攻击相关的节点。通过攻防图计算出 APT 攻击对无线通信网络的损害程度,构建最优主动防御决策模型,在保证无线通信网络安全性的前提下,提高攻击数据包拒包率和吞吐量,具备更好的防御效果。

构建无线通信网络最优主动防御决策模型流程如图 1 所示。

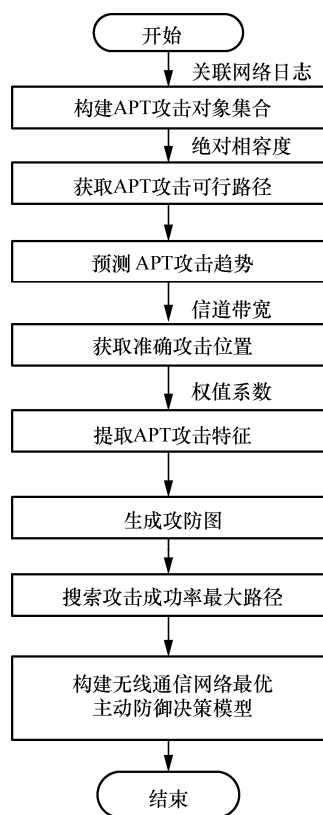


图 1 构建无线通信网络最优主动防御决策模型流程

1.1 预测 APT 攻击趋势

APT 攻击具有隐蔽性和持久性等特点,以获取敏感信息、控制资源、进行间谍活动或破坏关键基础设施。APT 攻击给受攻击的目标带来严重的数据泄露、业务中断、威胁情报、品牌声誉损害和经济损失等危害。在无线通信网络中,90% 的 APT 攻击都得到了有效控制,并留下了存档,因此攻击者在对网络攻击过程中,会留下攻击证据^[6]。APT 攻击趋势如图 2 所示。

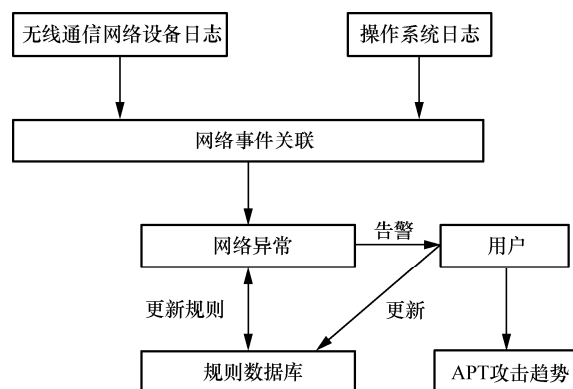


图 2 APT 攻击趋势

定义 $X_i = \{x_i^1, \dots, x_i^{a_i}, \dots\}$ 为 APT 攻击趋势预测中第 i 个来源的全部日志,各个日志在无线通信网络中的关联函数为:

$$L(x_i^{a_i}, x_j^{a_j}) = \begin{cases} 1, & \left(F(\varepsilon(x_i^{a_i}), \varepsilon(x_j^{a_j})) \right) = \text{true} \\ 0, & \text{其他} \end{cases} \quad (1)$$

其中, x_i^j 代表第 i 个来源中的第 j 个日志, $\varepsilon(x_j^{a_j})$ 代表日志 $x_j^{a_j}$ 的属性, $F(\varepsilon(x_i^{a_i}), \varepsilon(x_j^{a_j}))$ 代表属性 $\varepsilon(x_i^{a_i})$ 与属性 $\varepsilon(x_j^{a_j})$ 相同。

利用关联规则收集无线通信网络日志与 APT 攻击目标^[7],对网络中不同的日志进行关联,关联形式为:

$$G = \{X_i, Q, T_x, \mathcal{G}_{\text{APT}}, D^*\} \quad (2)$$

其中, Q 代表网络中不同日志的关联规则, T_x 代



表网络日志的有效期限, $\mathcal{G}_{\text{APT}}$ 代表无线通信网络对 APT 攻击的信任程度, D^* 代表无线通信网络遭受的 APT 攻击对象。

通过无线通信网络日志的关联, 可以明确 APT 攻击对象 D^* , 构建 APT 攻击对象集合, 表示为:

$$D^* = \{D_1^*, D_2^*, \dots\} \quad (3)$$

在无线通信网络中, 通过对不同来源的日志数据进行互相关联, 构建日志上下文的关联模型, 将关联模型与规则数据库中的日志数据配准^[8], 识别出无线通信网络遭受的 APT 攻击事件。

根据 APT 攻击证据, 对 APT 攻击对象的可信度进行融合处理^[9], 计算得到无线通信网络与 APT 攻击的反馈相容系数, 计算式为:

$$Q_{ij} = \frac{\partial_i(g_k)\partial_j(g_k)}{(\partial_i(g_k)\partial_i(g_k) + \partial_j(g_k)\partial_j(g_k))/2} \quad (4)$$

其中, g_k 代表第 k 个 APT 攻击事件, $\partial_i(g_k)$ 代表第 i 层无线通信网络日志中网络设备对第 k 个 APT 攻击事件的可信度。

利用反馈相容系数, 计算出 APT 攻击事件 g_k 在无线通信网络中的绝对相容度, 计算式为:

$$H_i(g_k) = Q_{ij}(g_k) \times T_i \quad (5)$$

其中, T_i 代表第 i 个无线通信网络日志的记录时间。

根据 APT 攻击事件 g_k 在无线通信网络中的绝对相容度, 更新无线通信网络设备对 APT 攻击事件的可信度^[10], 获取 APT 攻击的可行路径, 即:

$$\partial_i(g_k)_{\text{new}} = \omega_i \partial_i(g_k) H_i(g_k) \quad (6)$$

其中, ω_i 代表 APT 攻击对象在无线通信网络中的权重值。

通过对无线通信网络日志的关联, 构建 APT 攻击对象集合, 利用反馈相容系数, 计算出 APT 攻击事件在无线通信网络中的绝对相容度, 根据 APT 攻击的可行路径, 预测了 APT 攻击趋势。

1.2 提取无线通信网络的 APT 攻击特征

根据 APT 攻击趋势, 计算 APT 攻击源对无线通信网络攻击的信道带宽, 计算式为:

$$K_s = V_b f \quad (7)$$

其中, V_b 代表数据在无线通信网络中的传输速率, f 代表信道频率。

由于 APT 攻击信号具有时变性^[11], 需要准确获取无线通信网络受到 APT 攻击的位置, 即:

$$g(t) = \sqrt{\phi} f(G[t - t^0]) K_s \quad (8)$$

其中, ϕ 代表无线通信网络受到攻击的尺度因子, t^0 代表 APT 攻击时延。

基于无线通信网络受到 APT 攻击的位置, 计算出无线通信网络节点的权值系数, 计算式为:

$$\varpi = \sum_{k=1}^p u_k \chi_k + \sum_{k=p+1}^q h_k \chi_k \quad (9)$$

其中, u_k 代表正常节点的权值, χ_k 代表攻击节点的位置, h_k 代表攻击节点的权值。

为了准确提取出无线通信网络 APT 攻击特征, 得到攻击节点特征的提取残差参数:

$$\mu^2(p) = G[(\hat{\varpi} - \varpi)(\hat{\varpi} - \varpi)^T] \quad (10)$$

其中, $\hat{\varpi}$ 代表无线通信网络节点的特征分量。

当 $h_k = \hat{\varpi} \chi_k^T$ 时, 无线通信网络攻击特征的提取误差就会达到最小^[12], 存在:

$$\mu^2(p) = \sum_{k=p+1}^q G[(u_k - h_k)^2] = \sum_{k=p+1}^q \chi_k^T \Lambda^* \chi_k \quad (11)$$

其中, Λ^* 代表无线通信网络不同节点之间的特征值。

为了使 APT 攻击特征提取误差最小, 即当 $\mu^2(p) = 0$ 时, 提取出无线通信网络的 APT 攻击特征, 表示为:

$$u^2(p) = (1 - \Lambda^*) \sum_{k=p+1}^q \ell_k \quad (12)$$

其中, ℓ_k 代表无线通信网络的 APT 攻击特征。

基于 APT 攻击源对无线通信网络攻击的信道带宽, 获取无线通信网络受到 APT 攻击的位置, 利用无线通信网络节点的权值系数, 计算攻击节点特征的提取残差参数, 提取出无线通信网络的 APT 攻击特征。

1.3 构建无线通信网络最优主动防御决策模型

以提取出无线通信网络的 APT 攻击特征为依据, 构建无线通信网络最优主动防御决策模型, 防御 APT 攻击对无线通信网络的危害, 针对无线通信网络生成攻防图, 表示为:

$$R_E = \frac{Z_g \times Z_o}{A \times Y} \times b_j + q_s \quad (13)$$

其中, Z_g 代表 APT 攻击目标的状态集合, A 代表应用程序的状态节点集合, Z_o 代表网络初始安全状态, Y 代表网络安全状态的跳跃式过程, b_j 代表主机节点名, q_s 代表 APT 攻击在主机节点的权限。

利用攻防图^[13], 计算出 APT 攻击对无线通信网络的损害程度, 即:

$$S = \frac{w_i \cdot f(x)}{E(a, b)} \times C_g \quad (14)$$

其中, w_i 代表网络安全属性的权重, $f(x)$ 代表防御决策的隶属度函数, $E(a, b)$ 代表最优主动防御决策的期望收益, C_g 代表网络的机密性代价。

根据式 (14) 可以看出, APT 攻击会对无线通信网络产生一定损害^[14], 必须在网络安全状态下, 构建无线通信网络最优主动防御决策模型, 因此, 定义了无线通信网络的安全状态, 表示为:

$$A_z = \frac{ID_v \times ID_c}{S_e \times B_j} \times X_{APT} + \gamma \quad (15)$$

其中, ID_v 代表网络安全状态的迁移序列号, ID_c 代表 APT 攻击节点编号, S_e 代表网络受攻击后的损害, B_j 代表受攻击的网络主机标识, X_{APT} 代表攻击序列, γ 为防御攻击的措施。

无线通信网络在安全状态下时, 根据 APT 攻击趋势^[15], 搜索攻击成功率最大的路径, 即:

$$F_j = \frac{\alpha_j \cdot S_f}{W_s \times S_p} \times \lambda_s \quad (16)$$

其中, S_f 代表网络脆弱性节点受到攻击后的损害, W_s 代表网络损害值变量, λ_s 代表网络机密性的损害系数, α_j 代表 APT 攻击路径的损害程度, S_p 代表 APT 攻击趋势中某一次攻击对网络的损害。

在式 (16) 的路径上, 获取最容易受到攻击的节点之后, 构建无线通信网络最优主动防御决策模型, 计算式为:

$$F_Y = \frac{\xi \times A_z \times R_E}{\sigma_d \times F_j} + J^* \quad (17)$$

其中, ξ 代表攻击路径的成功概率, σ_d 代表 APT 攻击路径的危害系数, J^* 代表无线通信网络中主机信息的机密价值。

综上所述, 利用攻防图, 计算出 APT 攻击对无线通信网络的损害程度, 通过定义无线通信网络的安全状态, 搜索攻击成功率最大的路径, 构建了无线通信网络最优主动防御决策模型。

参数明细见表 1。

2 实验对比分析

2.1 实验平台

为了验证文中模型在无线通信网络主动防御决策中的效果, 设计了 APT 攻击 (钓鱼攻击、水坑攻击、远程执行代码攻击和侧信道攻击) 下的无线通信网络最优主动防御决策模型对比实验, 采用处理器为 Intel Core2 Duo E8400 (6 MB 高速缓存, 3.00 GHz, 1 333 MHz 前端总线) 的计算机。其中 3 台设备分别为 Web 服务器、FTP 服务器、APT 攻击服务器。由于防火墙的存在, APT 攻击服务器对 DMZ 中的 Web 服务器仅有最低的远程访问特权, DMZ 与内网通信, Web 服务器仅能被动接受服务请求。根据无线通信网络的攻防结构, 搭建了防御路径模拟平台, 如图 3 所示。



表 1 参数明细

参数	含义	参数	含义	参数	含义
$X_i = \{x_i^1, \dots, x_i^a, \dots\}$	关联函数	$f(x)$	隶属度函数	ϕ	尺度因子
$\varepsilon(x_j^{a_j})$	属性	C_g	机密性代价	ϖ	权值系数
T_x	有效期限	ID_c	节点编号	χ_k	位置
D^*	攻击对象	B_j	主机标识	$\hat{\sigma}$	特征分量
v_i	可信度	γ	措施	Λ^*	特征值
$\partial_i(g_k)$	可信度	S_f	损害	R_E	攻防图
T_i	记录时间	λ_s	损害系数	A	状态节点集合
ω_i	权重值	S_p	损害	Y	跳跃式过程
V_b	传输速率	ξ	成功概率	q_s	节点权限
$g(t)$	攻击位置	J^*	机密价值	w_i	权重
t^0	攻击时延	x_i^j	日志	$E(a, b)$	期望收益
u_k	权值	Q	关联规则	ID_v	迁移序列号
h_k	权值	$\mathcal{G}_{APT}$	信任程度	S_e	损害
$\mu^2(p)$	残差参数	Q_{ij}	反馈相容系数	X_{APT}	攻击序列
ℓ_k	攻击特征	g_k	攻击事件	F_j	最大路径
Z_g	状态集合	$H_i(g_k)$	绝对相容度	W_s	损害值变量
Z_o	初始安全状态	$\partial_i(g_k)_{new}$	可行路径	α_j	损害程度
b_j	主机节点名	K_s	信道带宽	F_V	最优主动防御决策模型
S	损害程度	f	信道频率	σ_d	危害系数

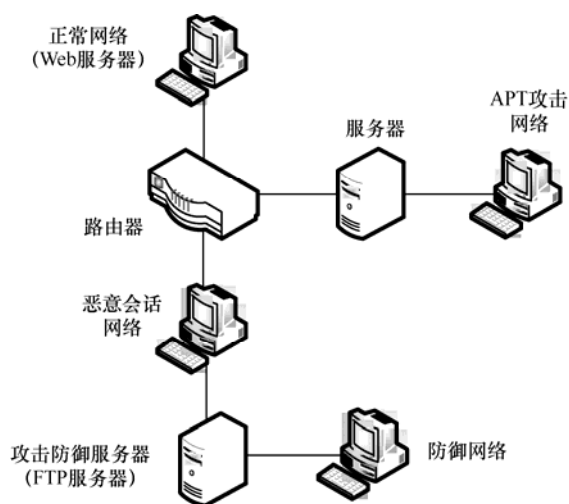


图 3 防御路径模拟平台

利用图 3 的实验平台，对 APT 攻击下无线通信网络进行主动防御模拟。使用 Weka 加载和分析

无线通信网络日志数据，应用关联分析算法构建 APT 攻击对象集合。利用 Python 及 Pandas 计算反馈相容系数，并分析和计算 APT 攻击事件在无线通信网络中的关联程度。使用 Sniffer 实时监测和分析无线信号传输，获取受到 APT 攻击的位置信息。利用 Aircrack-ng 对无线通信网络中的信号进行监测、分析和数据采集。使用 NetworkX 构建无线通信网络的攻防图，利用 MATLAB 计算攻防图中的指标和度量，综合考虑多个指标（如攻击数据包拒包率和吞吐量），以评估 APT 攻击对无线通信网络的损害程度。使用 MATLAB 构建最优主动防御决策模型，考虑不同防御策略的评估和选择。其中，反馈相容系数为[0,1]，Web 服务器权值系数为 0.8，FTP 服务器权值系数为 0.6。

2.2 测试对象

本文选择 APT 攻击服务器对无线通信网络中的不同应用程序进行攻击，并分别对其日志进行分析并统计，得出了无线通信网络应用程序的参数，见表 2。

表 2 无线通信网络应用程序的参数

应用程序名称	代码行数/行	APT 攻击数量/个
A	1 758	6
B	4 563	14
C	9 873	32
D	24 561	68
E	42 389	72
F	57 636	108
G	62 798	165
H	99 876	214

将表 2 中 8 个应用程序的各项参数导入图 3 的实验平台中，在 APT 攻击下，测试无线通信网络的主动防御效果。

2.3 APT 攻击检测

当无线通信网络的应用程序受到 APT 攻击之后，应用程序就会出现误码的现象，因此利用文中模型检测表 2 中 8 个应用程序的 APT 攻击，测试了应用程序现象，统计攻击对象的误码数量，并根据总代码数计算出误码率，应用程序的误码率如图 4 所示。

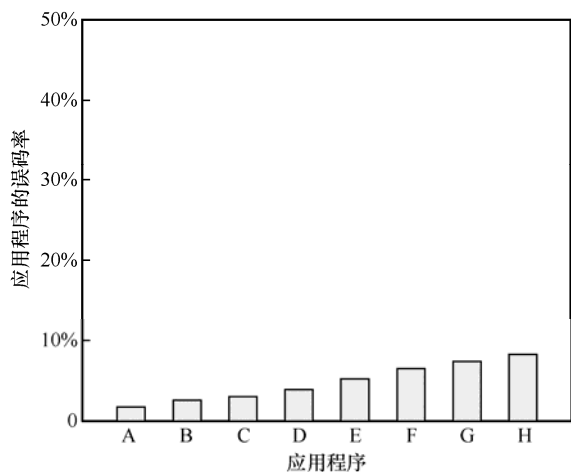


图 4 应用程序的误码率

根据图 4 的结果可知，随着 APT 攻击数量的增加，应用程序的误码率逐渐增大，说明本文模型能够检测到应用程序中的 APT 攻击。

2.4 性能对比

在性能对比测试中，引入轻量级系统 ScatterID 技术^[2]、最优种子调度策略算法^[3]、基于非零和随机博弈的防御决策模型^[4]和基于不完全信息博弈的防御决策模型^[5]与本文模型作对比，分别测试了无线通信网络的攻击数据包拒包率、吞吐量和时延，无线通信网络的攻击数据包拒包率如图 5 所示。

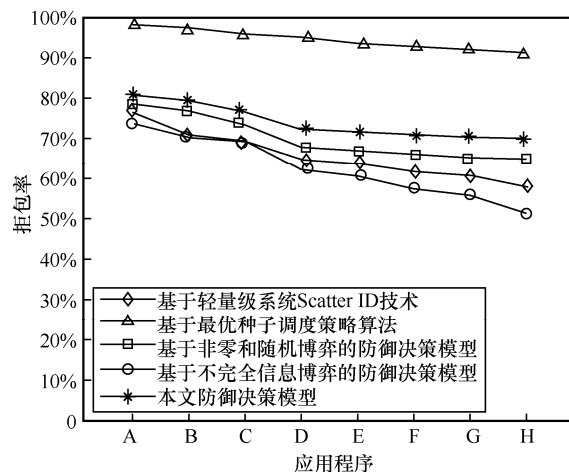


图 5 无线通信网络的攻击数据包拒包率

图 5 的结果显示，随着 APT 攻击数量的增加，无线通信网络的攻击数据包拒包率逐渐变小，采用轻量级系统 ScatterID 技术、最优种子调度策略算法、基于非零和随机博弈的防御决策模型和基于不完全信息博弈的防御决策模型对无线通信网络进行主动防御之后，拒包率在 50%~80%。而采用所提模型防御 APT 攻击时，各个应用程序对 APT 攻击的拒包率在 90% 以上，能够有效拒绝 APT 攻击访问网络，具有更好的防御效果。

无线通信网络的吞吐量如图 6 所示。根据图 6 的结果可知，轻量级系统 ScatterID 技术、最优种子调度策略算法、基于非零和随机博弈的防御决策模型和基于不完全信息博弈的防御决策模型受



到 APT 攻击的影响较大,导致应用程序吞吐量低于 10 000 bit/s,随着 APT 攻击数量的增加,应用程序在响应过程中的吞吐量逐渐变小,无法满足无线通信网络的高效运行需求。采用所提模型时,随着 APT 攻击数量的增加,虽然各个应用程序的吞吐量同样减小,但是始终在 16 000 bit/s 以上,说明文中模型对无线通信网络进行主动防御之后,可以保证网络的流畅性。

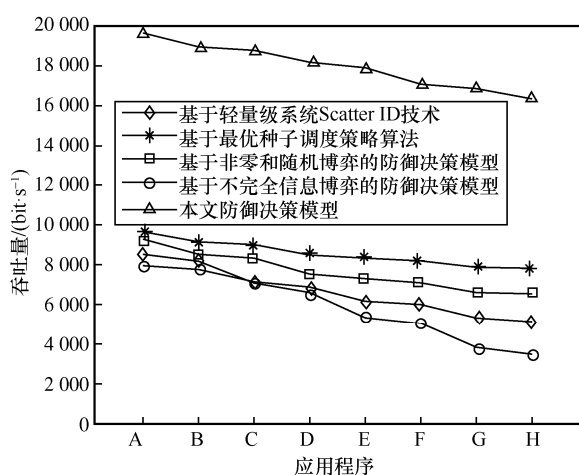


图6 无线通信网络的吞吐量

根据表3的结果可知,随着 APT 攻击数量的增加,各个防御方法的平均时延也有所增加。采用轻量级系统 ScatterID 技术、最优种子调度策略算法、基于非零和随机博弈的防御决策模型和基于不完全信息博弈的防御决策模型对无线通信网络进行主动防御之后,时延在 50~80 ms。而采用本文模型防御 APT 攻击时,时延在 45~55 ms,说明所提模型在保护无线通信网络免受 APT 攻击方面表现较好,具有高效的防御能力。

3 结束语

本文在 APT 攻击下提出了无线通信网络最优主动防御决策模型,实验结果表明如下。

(1) APT 攻击数量与应用程序的误码率成正比,本文模型可以准确检测到应用程序中的 APT 攻击。

(2) APT 攻击时,无线通信网络的攻击数据包拒包率在 90%以上,有效地防御了 APT 攻击访问网络,并提高了原有的防御效果。

(3) APT 攻击时,各个应用程序的吞吐量保持在 16 000 bit/s 以上,在对无线通信网络进行主动防御之后,保证了网络流畅运行。

(4) APT 攻击时,本文算法的时延较低,保证了无线通信网络的实时性和快速响应能力。

因此,该方法对 APT 攻击产生的误码率、APT 攻击的拒包率、网络吞吐量和时延方面均具有更好的防御效果,但是本文的研究还存在很多不足,在今后的研究中,希望可以引入演化博弈模型,体现攻防的随机性,提高对网络攻击防御的准确性。

参考文献:

- [1] 胡永进,马骏,郭渊博,等. 基于多阶段网络欺骗博弈的主动防御研究[J]. 通信学报, 2020, 41(8): 32-42.
HU Y J, MA J, GUO Y B, et al. Research on active defense based on multi-stage cyber deception game[J]. Journal on Communications, 2020, 41(8): 32-42.
- [2] HUANG Y, WANG W, JIANG T, et al. Detecting colluding sybil attackers in robotic networks using backscatters[J]. IEEE/ACM Transactions on Networking, 2021, 29(2): 793-804.
- [3] CHEN Z X, LU Y Q, QIN J C, et al. An optimal seed scheduling strategy algorithm applied to cyberspace mimic defense[J].

表3 无线通信网络的时延

APT 攻击数量/个	基于轻量级系统 ScatterID 技术	最优种子调度 策略算法	基于非零和随机博弈 防御决策模型	基于不完全信息博弈防御 决策模型	文中防御决策 模型
10	60 ms	53 ms	55 ms	70 ms	45 ms
20	65 ms	57 ms	61 ms	76 ms	49 ms
30	70 ms	61 ms	66 ms	79 ms	53 ms
平均时延	65 ms	57 ms	60.7 ms	75 ms	49 ms

- IEEE Access, 2021(9): 129032-129050.
- [4] 李静轩, 朱俊虎, 邱菡, 等. 基于非零和随机博弈的 APT 攻击主动防御策略选取[J]. 计算机应用研究, 2020, 37(10): 3071-3076, 3111.
LI J X, ZHU J H, QIU H, et al. Active defense strategy selection for anti-APT attack based on non-zero-sum stochastic game[J]. Application Research of Computers, 2020, 37(10): 3071-3076, 3111.
- [5] 王增光, 卢昱, 李玺. 基于不完全信息博弈的军事信息网络主动防御策略选取[J]. 兵工学报, 2020, 41(3): 608-617.
WANG Z G, LU Y, LI X. Active defense strategy selection of military information network based on incomplete information game[J]. Acta Armamentarii, 2020, 41(3): 608-617.
- [6] 王小平, 周问, 刘博. 三体对抗策略的预警机主动防御最优协同制导算法[J]. 空军工程大学学报(自然科学版), 2020, 21(2): 16-23.
WANG X P, ZHOU W, LIU B. A design of active defense optimal collaborative guidance algorithm for active defense of early warning aircraft based on three-body confrontation strategy[J]. Journal of Air Force Engineering University (Natural Science Edition), 2020, 21(2): 16-23.
- [7] 黄万伟, 袁博, 王苏南, 等. 基于非零和信号博弈的主动防御模型[J]. 郑州大学学报(工学版), 2022, 43(1): 90-96.
HUANG W W, YUAN B, WANG S N, et al. Proactive defense model based on non-zero-sum signal game[J]. Journal of Zhengzhou University (Engineering Science), 2022, 43(1): 90-96.
- [8] 田锋, 周安民, 刘亮, 等. ARS: 基于文件行为的勒索软件主动防御技术研究[J]. 四川大学学报(自然科学版), 2021, 58(2): 97-105.
TIAN F, ZHOU A M, LIU L, et al. ARS: research on proactive defense technology of ransomware based on file behavior[J]. Journal of Sichuan University (Natural Science Edition), 2021, 58(2): 97-105.
- [9] 王丹妮, 陈伟, 羊洋, 等. 基于高斯增强和迭代攻击的对抗训练防御方法[J]. 计算机科学, 2021, 48(S1): 509-513, 537.
WANG D N, CHEN W, YANG Y, et al. Countermeasure training defense method based on Gaussian enhancement and iterative attack[J]. Computer Science, 2021, 48(S1): 509-513, 537.
- [10] 尚立, 陈明, 张磊, 等. SDN 中基于机器学习的 DDoS 攻击协同防御[J]. 电力系统保护与控制, 2021, 49(16): 170-176.
SHANG L, CHEN M, ZHANG L, et al. Cooperative defense of DDoS attack based on machine learning in SDN[J]. Power System Protection and Control, 2021, 49(16): 170-176.
- [11] 谢升旭, 魏伟, 邢长友, 等. 面向 SDN 拓扑发现的 LDoS 攻击防御技术研究[J]. 计算机工程与应用, 2020, 56(10): 88-93.
XIE S X, WEI W, XING C Y, et al. Research on LDoS attack defense technology for SDN topology discovery[J]. Computer Engineering and Applications, 2020, 56(10): 88-93.
- [12] 蒋跃宇, 承昊新, 王康, 等. PLC-RF 无线传输网络中的能效最优设计方法[J]. 电信科学, 2023, 39(4): 111-119.
JIANG Y Y, CHENG H X, WANG K, et al. Design method of energy efficiency optimization in PLC-RF wireless transmission networks[J]. Telecommunications Science, 2023, 39(4): 111-119.
- [13] 顾泽宇, 张兴明, 魏帅. 基于增强学习的自适应动态防御机制[J]. 小型微型计算机系统, 2019, 40(2): 401-406.
GU Z Y, ZHANG X M, WEI S. Adaptive dynamic defense mechanism based on reinforcement learning[J]. Journal of Chinese Computer Systems, 2019, 40(2): 401-406.
- [14] 李元诚, 杨珊珊. 基于改进自注意力机制生成对抗网络的智能电网 GPS 欺骗攻击防御方法[J]. 电力自动化设备, 2021, 41(11): 100-106.
LI Y C, YANG S S. Defense method of smart grid GPS spoofing attack based on improved self-attention generative adversarial network[J]. Electric Power Automation Equipment, 2021, 41(11): 100-106.
- [15] 王增光, 卢昱, 李玺. 多阶段信号博弈的装备保障信息网络主动防御[J]. 火力与指挥控制, 2020, 45(12): 142-148.
WANG Z G, LU Y, LI X. Research on active defense of equipment support information network based on multi-stage signaling game[J]. Fire Control & Command Control, 2020, 45(12): 142-148.

[作者简介]



孟勤 (1991—), 男, 国网辽宁省电力有限公司信息通信分公司工程师, 主要研究方向为网络安全防御决策、漏洞挖掘等。



王丹妮 (1986—), 女, 国网辽宁省电力有限公司信息通信分公司高级工程师, 主要研究方向为网络安全前沿技术、技防体系建设等。



吕军 (1987—), 男, 国网辽宁省电力有限公司信息通信分公司高级工程师, 主要研究方向为网络与信息安全。



张福良 (1989—), 男, 国网辽宁省电力有限公司信息通信分公司高级工程师, 主要研究方向为数据挖掘与分析。