doi:10.11959/j.issn.1000-436x.2017204

基于攻击预测的网络安全态势量化方法

胡浩[1,2]，叶润国[3]，张红旗[1,2]，杨英杰[1,2]，刘玉岭[4]

（1. 解放军信息工程大学三院，河南 郑州 450001；2. 河南省信息安全重点实验室，河南 郑州 450001；
3. 中国电子技术标准化研究院，北京 100007；4. 中国科学院软件研究所可信计算与信息保障实验室，北京 100190）

摘 要：为准确、全面地预测攻击行为并量化攻击威胁，提出一种基于攻击预测的安全态势量化方法。通过融合攻击方、防御方和网络环境态势要素，依据实时检测的攻击事件评估攻击者能力和漏洞利用率，并计算攻防期望耗时；进而设计基于动态贝叶斯攻击图的攻击预测算法，推断后续攻击行为；最后从主机和网络这 2 个层面将攻击威胁量化为安全风险态势。实例分析表明，该方法符合实际对抗网络环境，能够准确预测攻击发生时间并合理量化攻击威胁。

关键词：攻击预测；安全态势；贝叶斯攻击图；攻防对抗；时间预测

中图分类号：TP393.8 **文献标识码**：A

Quantitative method for network security situation based on attack prediction

HU Hao[1,2], YE Run-guo[3,4], ZHANG Hong-qi[1,2], YANG Ying-jie[1,2], LIU Yu-ling[4]

(1. The Third Institute, PLA Information Engineering University, Zhengzhou 450001, China;
2. Henan Key Laboratory of Information Security, Zhengzhou 450001, China;
3. China Electronics Standardization Institute, Beijing 100007, China;
4. Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)

Abstract: To predict the attack behaviors accurately and comprehensively as well as to quantify the threat of attack, a quantitative method for network security situation based on attack prediction was proposed. By fusing the situation factors of attacker, defender and network environment, the capability of attacker and the exploitability rate of vulnerability were evaluated utilizing the real-time detected attack events, and the expected time-cost for attack-defense were further calculated. Then an attack prediction algorithm based on the dynamic Bayesian attack graph was designed to infer the follow-up attack actions. At last, the attack threat was quantified as the security risk situation from two levels of the hosts and the overall network. Experimental analysis indicates that the proposed method is suitable for the real adversarial network environment, and is able to predict the occurrence time of attack accurately and quantify the attack threat reasonably.

Key words: attack prediction, security situation, Bayesian attack graph, attack-defense, time prediction

1 引言

随着信息技术的迅猛发展，网络空间安全面临的攻击与威胁日益增多，而传统安全产品越来越无法满足防护需求，网络安全态势感知（NSA, network security situation）作为一种新的网络安全防护手段，

收稿日期：2017-03-02；**修回日期**：2017-08-28

基金项目：国家高技术研究发展计划（“863”计划）基金资助项目（No.2012AA012704, No.2015AA016006）；国家重点研发计划课题基金资助项目（No.2016YFF0204003）；郑州市科技领军人才基金资助项目（No.131PLJRC644）；“十三五”装备预研领域基金资助项目（No.61400020201）；CCF-启明星辰“鸿雁”科研计划基金资助项目（No.2017003）；公安部信息网络安全重点实验室开放课题基金资助项目（No.C15604）

Foundation Items: The National High Technology Research and Development Program of China (863 Program) (No.2012AA012704, No.2015AA016006), The National Key Research and Development Program of China (No.2016YFF0204003), The Science and Technology Leading Talent Project of Zhengzhou (No.131PLJRC644), The Equipment Pre-Research Foundation During the 13th Five-Year Plan Period (No.61400020201), The CCF-Venus “Hongyan” Research Plan (No.2017003), The Key Lab of Information Network Security, Ministry of Public Security (No.C15604)

实现在复杂变化的网络环境中认知、理解并预测网络的安全状态及其发展趋势，有助于管理人员及时掌握网络安全状况，并对未来可能出现的威胁作出有效预测，成为近年来的一个研究热点。态势预测作为态势感知的重要组成部分，用于分析网络安全的变化趋势，为安全防护提供决策支持，引起了国内外学者的广泛关注，现有网络安全态势预测方法主要分为以下 3 种。

基于时空序列的方法。该方法的假设条件为安全态势值的变化具有规则和周期性，通过分析安全态势的前后依赖关系，实现对网络安全趋势的预测。Qu 等[1]提出了一种基于 D-S 证据理论的态势预测方法，通过融合多源报警信息分析网络安全态势，然而由于证据理论在多证据合成时存在悖论问题，导致预测结果准确度不高。吕慧颖等[2]通过分析威胁事件的渗透过程和转移规则，在时间和空间维度上对威胁进行关联，建立关联模式库，能够实时预测攻击意图，并推测攻击路径。然而由于网络攻防过程的动态性，导致攻击图节点概率不能客观反映攻防双方的对抗状态，从而影响攻击路径预测的准确性。针对此情况，席荣荣等[3]基于报警统计特征，提出了改进报警数据源有效性的方法，提高了预测结果的准确性，但只分析一个采样周期内的报警信息，适用于短期预测。文献[4]提出一种面向多步攻击的网络安全态势评估，通过对攻击场景进行关联分析，识别攻击轨迹与攻击阶段，并对当前网络安全状态进行了评估，但缺乏对未来趋势的预测。刘玉岭等[5]进一步融合攻击方、防护方和网络环境信息，提取网络安全态势要素，提高了预测结果的准确性，但未对态势变化的时间节点进行量化分析。自回归移动平均模型（ARIMA, autoregressive integrated moving average model）[6]和指数平滑（ES, exponential smoothing）方法[7]是 2 种通用的时间序列预测方法，但主要适用于分析平稳时间序列的变化规律，当应用于实际网络时，由于各种安全事件突发，因此预测效果不佳。

基于图论的方法。该方法利用网络环境中的脆弱性信息生成状态转移图，并从攻击者角度出发，依据当前状态对网络未来可能出现的安全状况进行预测。文献[8]利用时间自动机描述脆弱性状态迁移过程，依据节点状态和节点间依赖关系预测攻击成功概率，分析不同攻击意图的概率随时间的变化趋势。陈小军等[9]在攻击图模型中引入转移概率表，利用累积概率计算目标攻击节点的最大可达概率，用来识别攻击意图和预测攻击路径，辅助威胁态势的研究。Liu 等[10]引入隐马尔可夫模型，结合报警观测序列，利用 Viterbi 算法推导最大可能状态转移序列，实现攻击意图识别，但缺乏全网风险值量化。Dai 等[11]综合考虑网络防御措施，量化攻击成本与收益，建立风险流攻击图模型，利用模糊综合评估法计算不同入侵路径的风险饱和率并对路径的威胁进行排序。Fredj 等[12]利用吸收马尔可夫链描述攻击图中的状态转移行为，通过报警关联，实现攻击识别、分析与预测，但预测结果仅建立在当前状态的基础上，未与历史攻击行为相结合，有效性还有待进一步评估。Abraham 等[13]通过引入漏洞生命周期，分析攻击路径长度随漏洞发布时间的变化规律。Ghasemigol 等[14]针对攻击发生概率的不确定性，提出了一种综合预测算法，提高了预测精度。事实上，以上方法主要针对攻击预测展开研究，包括攻击意图、路径和概率，但未全面量化攻击威胁对网络安全态势的影响。

基于博弈论的方法。该方法在攻防对抗环境中，利用博弈理论预测攻防双方的下一步动作进而分析网络的安全态势，在态势要素选择上较为全面。Wang 等[15]利用网络连接信息和脆弱性信息，基于随机 Pertri 网构建了攻防博弈模型，对攻击成功率、可能路径和平均攻击时间进行了分析。张勇等[16]通过分析威胁传播规律，构造威胁传播网络，建立威胁、管理员和用户三方参与的博弈分析模型，分析安全威胁的演化趋势。Chen 等[17]通过数据融合建立马尔可夫博弈模型，提出了威胁预测和态势感知方法。Wu 等[18]提出了基于大数据分析的电网系统安全态势感知机制，将模糊聚类和博弈论相结合，提高预测效率并降低错误率。Serra 等[19]从防御者角度出发，借助帕累托最优化方法，折中考虑了防御成本与防御收益。博弈论方法在军事领域应用比较成熟，而网络的突发性强、不可预知因素多，因此对网络攻防建模难度较大，且上述方法主要预测未来一段或若干时段内的态势变化，未能量化具体时间。

通过上述分析，目前研究在以下 3 个方面仍有待改进：1) 预测过程对所有攻击者无差别处理，然而不同攻击者的实际漏洞利用能力不同，缺乏对攻击者的区分；2) 攻击预测集中于分析攻击意图、目标、路径和概率，缺乏对入侵时间的量化；3) 如何

合理地衡量攻击威胁对网络系统的影响，给出一种通用有效的安全态势量化标准还有待进一步研究。

为解决以上问题，本文提出一种基于攻击预测的网络安全态势量化方法。通过全方位融合攻击方、防御方和网络环境信息的态势要素，依据实时观测的攻击行为，推测攻击者的能力等级，区分不同攻击者，分析漏洞实际利用率，评估防御策略，计算攻防期望耗时；然后建立动态贝叶斯攻击图，结合网络攻防实时变化过程，判断攻击者能否在脆弱性修复之前完成状态转移，全面准确地预测后续攻击行为信息；进一步结合通用漏洞评分标准（CVSS, common vulnerability scoring system）[20]和网络资产信息，从主机和网络 2 个层面将攻击威胁映射为安全态势，实现对攻击威胁的合理量化，辅助管理员全面、准确地把握网络安全的变化趋势。

2 网络安全态势预测模型

网络安全态势取决于攻击方、防御方和环境信息的动态变化，任何一方的变动都会引起网络安全态势的变化，因此，对态势预测要素采集应尽量丰富。本节首先对相关术语进行定义，然后提出网络安全态势预测研究框架。

2.1 相关概念及描述

定义 1 原子攻击 a。指攻击者在网络中实施的单个攻击动作，其可能是对主机服务的扫描或对主机漏洞的一次利用，每个原子攻击动作 a 触发攻击者转移到一个攻击状态 S。

定义 2 攻击者能力水平。使用一个二元组 $\{ACAP, AMTI\}$ 表示，$ACAP$ 指攻击者的攻击能力等级，其中，$ACAP \in \{\text{Low}, \text{Medium}, \text{High}\}$，分别对应低、中、高 3 个能力等级，$AMTI$ 是指攻击者攻破一个漏洞的平均耗时，攻破利用率低的漏洞的平均耗时更长。

定义 3 贝叶斯攻击图 BAG。使用一个五元组 $\text{BAG} = (S, A, E, \xi, \Delta)$ 表示，其中，S 表示状态节点集合，A 表示原子攻击节点集合，E 表示有向边集合，ξ 表示状态间的依赖关系，Δ 表示原子攻击概率集合。

1) $S = \{S_1, S_2, \cdots, S_n\}$ 表示 n 个不同状态节点构成的集合，$\forall S_i \in S$，$p(S_i)$ 表示攻击者到达状态 S_i 的概率。

2) $E \subseteq A \times A$，$\forall e \in E$，$e = \text{pre}(a) \to a$，$\text{pre}(a)$ 为原子攻击 a 的前提攻击节点。

3) 对于 $\text{pre}(S) \to S$，$\text{pre}(S)$ 为状态节点 S 的起始状态节点，该状态转移依赖原子攻击 $a \in A$，$p(a) \in \Delta$，$p(a)$ 表示原子攻击 a 的发生概率。

4) $\forall S_i \in S$，$\exists \xi_i \in \xi$ 与 S_i 对应，满足 $\xi_i \in \{\text{AND}, \text{OR}\}$；其中，$\xi_i = \text{AND}$ 表示只有状态节点 S_i 的全部父节点全部入侵成功，状态节点 S_i 才有可能实现；$\xi_i = \text{OR}$ 表示只要状态节点 S_i 的任一父节点被成功入侵，S_i 就有可能实现，满足运算规则

$$p(S_i) = \begin{cases} \prod p(a_i)\, p(\text{pre}(S_i)), & \xi_i = \text{AND} \\ 1 - \prod \left[1 - p(\text{pre}(S_i))\, p(a_i)\right], & \xi_i = \text{OR} \end{cases}$$

其中，$\forall a_i \in a$。

定义 4 状态转移概率矩阵 ***SP***。将攻击图中的状态转移概率用邻接矩阵 ***SP*** 来表示，$\forall SP_{i,j} \in \boldsymbol{SP}$，$SP_{i,j}$ 表示状态转移 $S_i \to S_j$ 的概率，在数值上等于攻击依赖脆弱性 v 的利用率 $p(v)$；若状态转移不可达，令 $SP_{i,j} = 0$；同时，$SP_{i,i} = 1$。

定义 5 攻击期望耗时矩阵 ***AT***。表示攻击者入侵各状态节点的期望耗时，$\forall AT_{i,j} \in \boldsymbol{AT}$，$AT_{i,j}$ 表示 $S_i \to S_j$ 的期望耗时；若状态转移不可达，令 $AT_{i,j} = \infty$；同时，$AT_{i,i} = 0$。

定义 6 防御期望耗时矩阵 ***DT***。表示防御者修复各脆弱性所需的期望耗时，$\forall DT_{i,j} \in \boldsymbol{DT}$，$DT_{i,j}$ 表示防御者阻断 $S_i \to S_j$ 的期望耗时；若状态转移不可达，令 $DT_{i,j} = 0$；同时，$DT_{i,i} = 0$。

定义 7 状态转移关系矩阵 ***SD***。表示攻击图中状态转移的依存关系，$\forall QD_{i,j} \in \boldsymbol{SD}$，$QD_{i,j}$ 表示 $S_i \to S_j$ 的依存关系，令 $QD_{i,j} = \xi$，若不可达，令 $QD_{i,j} = \varnothing$；同时，$QD_{i,i} = \text{OR}$。

定义 8 状态发生概率向量 ***P***。表示攻击者转移到攻击图中不同状态节点的实现概率，$\forall P_i \in \boldsymbol{P}$，$P_i$ 表示攻击者转移到状态 S_i 的概率。

定义 9 状态发生时间向量 ***T***。表示入侵各状态节点的期望发生时间，$\forall T_i \in \boldsymbol{T}$，$T_i$ 表示攻击者到达状态 S_i 的时间。

攻击者对脆弱性的利用能力决定了状态转移的概率，如定义 2 所示；定义 4~定义 9 形式化描述了攻防安全态势要素信息，在态势要素的动态驱动下，攻击对抗活动依次展开，表现为攻击状态的变迁，攻击路径的转换；利用定义 3 的 BAG 模型可以模拟网络渗透过程，预测未来可能的攻击行为。

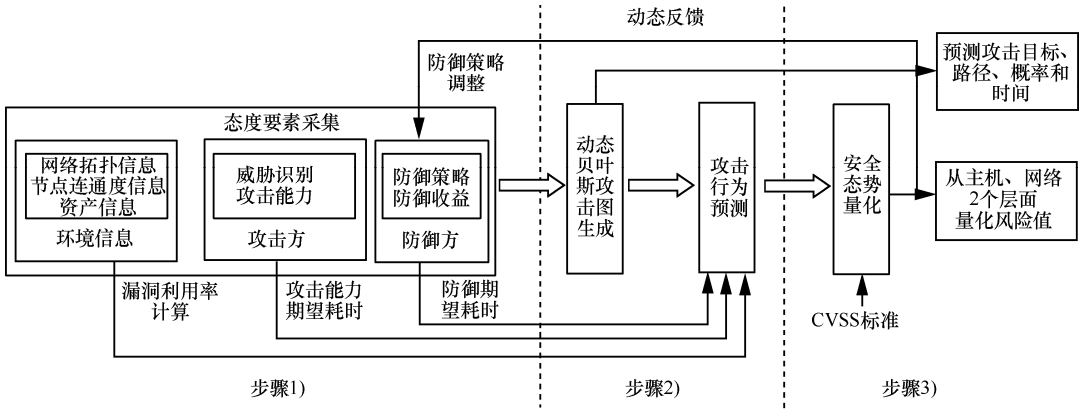


图 1　网络态势感知预测模型框架

2.2　网络安全态势感知预测框架

网络安全态势预测的整体框架如图 1 所示，基本思想是通过实时采集各种网络设备运行状况、网络行为以及用户行为信息，提取网络环境、攻击方和防御方的态势要素，通过分析当前网络“态”建立以攻击为驱动的贝叶斯攻击图模型，预测后续攻击行为，进一步结合 CVSS 量化未来网络安全变化的“势”。在攻防对抗过程中，“势”随着“态”的动态变化实时调整。具体实施步骤如下。

1) 网络安全态势要素采集

环境信息包括网络拓扑、连通性和漏洞信息等，其中，拓扑结构依据对网络结构的统计，网络连通性依据网络中防火墙的过滤规则，漏洞采集利用脆弱性扫描工具 Nessus，并通过查询美国国家漏洞数据库（NVD, national vulnerability database）得到漏洞信息。攻击方信息包括攻击能力、耗时和漏洞利用率等，来源于入侵检测系统、防火墙、主机审计日志等传感器的报警数据。防御方信息来源于防御策略集，包括漏洞修复、防火墙访问规则调整和安全配置更新等。

2) 网络攻击行为预测

根据采集到的攻击事件，评估攻击能力，分析漏洞利用率，计算攻击期望耗时，结合防御策略量化防御期望耗时，在此基础上，建立贝叶斯攻击图，当前研究者开发多种攻击图自动生成工具如 MulVal、TVA、NetSPA 等，本文选用开源的 MulVal 工具，生成的攻击图粒度为多项式级别，且为无环图，对后续攻击行为进行推演，预测攻击路径、概率和时间。随着攻防活动的深入，不断出现的状态变化可以验证预测算法的准确性，并作为新的网络安全态势要素进行下一轮的预测，具体攻击预测算法将于第 3 节详细介绍。

3) 网络安全态势量化

以攻击预测结果为基础，结合 CVSS 和网络资产信息，从主机、网络 2 个层面对安全态势进行量化。将抽象的攻击行为信息映射为定量的网络安全风险值，直观地表达当前网络系统面临的威胁及其演化趋势。具体方法将于第 4 节详细介绍。

3　网络攻击行为预测算法

本节首先证明对于同一漏洞，攻击能力与实际漏洞利用率符合正比关系，分析如何依据先验的攻击行为评估攻击者的能力等级，并结合攻击能力和漏洞复杂度评价漏洞利用率；接着结合漏洞利用率和先验攻击耗时计算攻击期望耗时；然后基于动态贝叶斯攻击图，提出攻击预测算法，最后分析算法的复杂度。

3.1　攻击者能力评估

CVSS 由美国国家基础建设咨询委员会发布，是漏洞评估的行业公开标准，CVSS 利用存取复杂度（AC, access complexity）来描述发动脆弱性利用的难度，分为 Low、Medium、High 这 3 个等级。本文利用脆弱点攻击难度作为参考依据，用于确定攻击者能力等级。一方面，取代传统的凭借主观经验确定攻击者水平的随意性，增强研究的通用性；另一方面，综合考虑攻击能力可以通过攻击事件反映，依据历史攻击事件的脆弱性利用难度衡量攻击能力，可以反映攻击者的真实水平，以区分不同的攻击者，定义攻击者的能力水平 $ACAP$ 等于其利用脆弱性的复杂度 AC，评估函数为

$$ACAP = \max\left(AC(Vuln)\right)$$

3.2 漏洞利用率分析

对同一漏洞，攻击能力越强，漏洞利用率越高，由贝叶斯公式可以得出以下结论。

定理 1 由同一漏洞的攻击结果推断攻击者能力等级的概率分布正比于其实施此次攻击成功或失败的概率分布。

证明 对于同一攻击行为 *Attack*，利用复杂度 *AC* 的漏洞 *Vuln* 的攻击结果 $Attack(Vuln)\in\{\text{succ},\text{fail}\}$，由该结果推断攻击能力的概率为 $p(ACAP\,|\,Attack(Vuln))$，假设攻击成功的概率为 $f\left(ACAP, AC\right)$，由贝叶斯公式可得

$$p\left(ACAP\,|\,Attack(Vuln)\right)=\frac{p\left(ACAP\right)p\left(Attack(Vuln)\,|\,ACAP\right)}{p\left(Attack(Vuln)\right)}$$

由于不同攻击能力 *ACAP* 的先验概率 $p(ACAP)$ 相等，且 $p\left(Attack(Vuln)\right)$ 为常数（由攻击结果统计得到），故 $p\left(ACAP\,|\,Attack(Vuln)\right)\propto p\left(Attack(Vuln)\,|\,ACAP\right)$。

当 $Attack(Vuln)=\text{succ}$ 时，$p\left(\text{succ}\,|\,ACAP\right)=f\left(ACAP, AC\right)$，故 $p\left(ACAP|\,\text{succ}\right)\propto f\left(ACAP, AC\right)$；当 $Attack(Vuln)=\text{fail}$ 时，$p\left(\text{fail}\,|\,ACAP\right)=1-f\left(ACAP, AC\right)$，因此，$p\left(ACAP|\,\text{fail}\right)\propto 1-f(ACAP, AC)$。

综上，得证。

在定理 1 的基础上结合 CVSS，定义不同等级攻击能力对漏洞的实际利用率如表 1 所示。

表 1 不同攻击能力的漏洞利用率

AC	$p(AC, ACAP)$		
	ACAP=Low	*ACAP*=Medium	*ACAP*=High
Low	0.5	0.7	0.9
Medium	0.3	0.5	0.7
High	0.1	0.3	0.5

从表 1 中可以看出，若漏洞复杂度 *AC* 相同，则攻击能力 *ACAP* 越高，漏洞利用率越高；在攻击能力 *ACAP* 不变的情况下，对于复杂度 *AC* 低的漏洞的利用率较高。

3.3 攻击期望耗时量化

针对利用率不等的漏洞，攻击耗时往往不等，对于利用率低的漏洞，其耗时越长。受攻击者自身因素的影响，其往往具有攻击习惯，通过分析先验攻击路径耗时，能在一定程度上推测后续攻击可能的期望耗时。对于已经发生的攻击事件，采用统计加权的方法衡量平均耗时。定义先验攻击耗时 $AMTI_{\text{prior}}$ 为

$$AMTI_{\text{prior}}=\frac{\sum_{i=1}^{q}\left[\left(t_{a_i}-t_{\text{pre}(a_i)}\right)p\left(v_i\right)\right]}{q-1}$$

其中，q 表示先验攻击路径 $\text{Path}_{\text{prior}}$ 的长度，t_{a_i} 表示攻击路径 $\text{Path}_{\text{prior}}=(a_1,a_2,\cdots,a_q)$ 中原子攻击动作 $a_i(1\leqslant i\leqslant q)$ 的发生时刻，其依赖漏洞 v_i 的利用率为 $p(v_i)$，$t_{\text{pre}(a_i)}$ 表示 a_i 的前提攻击 $\text{pre}(a_i)$ 的发生时刻。

在后续攻击过程中，攻击者入侵利用率 $p(v)$ 的漏洞 v 的期望耗时 $AMTI_{\text{expected}}$ 为

$$AMTI_{\text{expected}}=\frac{AMTI_{\text{prior}}}{p(v)}=\frac{\sum_{i=1}^{q}\left[\left(t_{a_i}-t_{\text{pre}(a_i)}\right)p\left(v_i\right)\right]}{(q-1)p(v)}$$

3.4 基于动态贝叶斯攻击图的攻击行为预测算法

首先基于网络环境信息，利用工具 MulVal 生成攻击图，其基本思想是通过对攻击能力与防御策略的评估，结合贝叶斯攻击图，动态关联攻防策略对路径选择的影响，判断攻击者能否在脆弱性修复之前完成状态转移，以攻击为驱动，模拟状态变迁过程，预测算法步骤如算法 1 所示。

算法 1 基于攻击图的攻击行为预测算法

输入 攻击图 $BAG=(S,A,E,\xi,\Delta)$

输出 攻击次数 *round*，攻击发生概率矩阵 $\boldsymbol{M}$ 和发生时间矩阵 $\boldsymbol{N}$

begin

1) 根据定义 4~定义 9 初始化 $r=0$, $SP, AT, DT, \boldsymbol{P}^r, \boldsymbol{T}^r$

2) for $i=1$ to n {

3) for $j=1$ to n {

4) if 状态转移 $S_i\rightarrow S_j$ 已经发生，更新 SP, AT, DT, $\boldsymbol{P}^r$, $\boldsymbol{T}^r=$真实值}}

5) for $i=1$ to n {

6) for $j=1$ to n {

7) if $T_i^r+AT_{i,j}>DT_{i,j}$ {更新 $SP_{i,j}=0$; break}

8) else 更新 $P_i^{r+1}=P_1^r\times SP_{1,i}\oplus P_2^r\times SP_{2,i}\oplus\cdots\oplus P_n^r\times SP_{n,i}$，记录 $M_{r+1,i}=P_i^{r+1}$

9)　　if $P_i^r \times SP_{i,j} > 0$，更新 $T_i^{r+1} = T_i^{r+1} + MaxAT_{i,j}$，记录 $N_{r+1,i} = T_i^{r+1}$

10)　　if $\{\sum_{k=1}^{n} SP_{k,i} = 1 \,\&\&\, i \neq j\}$ 更新 $SP_{i,j} = 0\}\}$

11)　　记录 $round = r$

12)　　当 $\boldsymbol{P}^{r+1} \neq \boldsymbol{P}^r$ 时，$r = r + 1$，转第 2)行

13) return $round$, $\boldsymbol{M}$, $\boldsymbol{N}$

end

在算法 1 中，第 1)行表示初始化过程，轮次计数器 $r = 0$ 表示网络初始状态；算法每执行完一轮，检测网络中是否有新的安全事件产生，如第 2)行~第 4)行所示，若观测到状态转移行为 $S_i \to S_j$，则将矩阵及向量相应位置上的元素值更新为实际值，如第 4)行所示。

第 5)~第 10)行表示递归过程，旨在分析可能的状态转移行为，一轮递归表示一次可能的原子攻击，对于每个状态节点 S_i，首先结合攻击与防御期望耗时，分析可能的转移路径 $S_i \to S_j$，若 $T_i^r + AT_{i,j}^r \geqslant DT_{i,j}^r$ 成立，表明在脆弱性修复之前，攻击者不能完成状态转移，因此 $S_i \to S_j$ 不可达，更新 $SP_{i,j}^r = 0$，跳出循环，如第 7)行所示；反之，则更新状态 S_i 的发生概率，并写入 $M_{r+1,i}$，如第 8)行所示，其中，$\oplus$ 的运算规则根据定义 3 的第 4 条；同时更新到达 S_j 的最近时间，并写入 $N_{r+1,i}$，如第 9)行所示，其中，$\max AT_{i,j}$ 表示到达 S_j 的最近时间；为保证攻击者不进行重复的状态迁移，将已经发生过且无其他路径可以利用的状态转移边删去，如第 10)行所示；递归完成后，记录最新轮次 $round = r$，如第 11)行所示。

第 12)行表示算法终止条件，即状态发生概率向量 $\boldsymbol{P}^r$ 趋于稳定，满足 $\boldsymbol{P}^{r+1} = \boldsymbol{P}^r$，此时输出攻击次数 $round$，状态发生概率矩阵 $\boldsymbol{M}$ 和发生时间矩阵 $\boldsymbol{N}$，其中，矩阵 $\boldsymbol{M}$ 和 $\boldsymbol{N}$ 的第 r 行分别代表执行 r 轮攻击后的状态发生概率向量 $\boldsymbol{P}^r$ 和时间向量 $\boldsymbol{T}^r$，算法结束。

关于算法 1 的 4 点补充说明如下。

1) 算法 1 定期检测网络中是否有新的安全事件产生，并动态更新攻防态势要素，当要素发生变化时重新执行此算法，因此具备良好的自适应特性。

2) 状态转移依据当前状态以及未来可能的攻击路径，由于攻击者对整体的网络信息并不熟悉，其近期入侵状态节点具有随机性，因此，一步转移选择最有可能实现的转移路径。

3) 动态贝叶斯攻击图是有向无环图，其预测过程是一个递归，因此从任意初始状态出发，最终均可以达到稳定状态。

4) $round$ 等于后续可能路径长度的预测值，通过筛选所有符合该长度的攻击路径，并匹配已知攻击序列，能够预测后续可能的攻击路径。

3.5　算法效能分析

1) 时间复杂度

算法是从每一个初始状态到稳定状态的所有路径的遍历，设状态数为 n，总路径数为 m，程序仅在攻防态势要素发生变化时才会运行，因此时间复杂度不大于 $O(mn)$。

2) 空间复杂度

算法需要维护 $n \times n$ 的状态转移概率矩阵 $\boldsymbol{SP}$，攻击期望耗时矩阵 $\boldsymbol{AT}$、防御期望耗时矩阵 $\boldsymbol{DT}$、状态转移关系矩阵 $\boldsymbol{SD}$ 和 r 对 $n \times 1$ 的状态发生概率向量 $\boldsymbol{P}$ 和时间向量 $\boldsymbol{T}$，且 $r \leqslant n$，因此空间复杂度不大于 $O(6n^2)$。

4　基于攻击预测的安全态势量化方法

本节从主机和网络 2 个层面结合 CVSS 标准将攻击威胁量化为安全态势。根据主机态势值高低，分析关键资产受威胁程度，根据全网态势值变化，掌握网络攻击的整体渗透进度，为网络监控和管理提供依据。

4.1　漏洞威胁影响度量

CVSS 给出了一种基于机密性、完整性、可用性这 3 个指标评价的漏洞威胁得分标准，用于衡量单个漏洞对网络的影响。其威胁得分为

$$Impact(v) = 10 \times \left(1 - (1 - C)(1 - I)(1 - A)\right)$$

其中，C、I、A 分别是机密性、完整性、可用性的威胁影响得分。

4.2　安全态势量化分析

安全态势可以借助安全风险值来量化，安全风险通过安全事件针对漏洞的风险级别来表征安全事件造成的损失，是衡量网络安全的重要指标。首先结合网络环境信息，利用工具 MulVal 生成攻击图，然后执行算法 1 预测攻击次数 $round$ 和状态发生概率矩阵 $\boldsymbol{M}$，最后综合漏洞威胁得分 $Impact$ 以及

主机节点权重值 *Weight*，计算该攻击场景的安全态势值 NSA。算法具体步骤如算法 2 所示。

算法 2 基于攻击预测的安全态势量化算法

输入

攻击次数 *round*，状态发生概率矩阵 ***M***，

各主机信息 $host_x=(h,s,g_x,Weight(x,y),Impact(v_y^x)),1\leqslant x\leqslant h,1\leqslant y\leqslant g_x$

输出

各轮次主机安全态势值矩阵 ***NSAH***，全网态势值向量 ***NSAN***

begin

1) 初始化 $r=0$

2) $Prob(\boldsymbol{M},r,v_y^x)$ 表示矩阵 ***M*** 中，第 *r* 轮攻击时利用漏洞 v_y^x 到达状态的发生概率

3) while $r\leqslant round$ do {

4) 计算 $Service_y$ 占主机 $host_x$ 的权重

$$Weight_{Service_y}=\frac{Weight(x,y)}{\sum_{y=1}^{g_x}Weight(x,y)}$$

5) 计算 $NSAH_{r,x}=\sum_{y=1}^{g_x}Prob(\boldsymbol{M},r,v_y^x)\cdot Impact(v_y^x)\left[\frac{Weight(x,y)}{\sum_{y=1}^{g_x}Weight(x,y)}\right]$

6) 计算 $NSAN_r=\sum_{x=1}^{h}\sum_{y=1}^{g_x}Prob(\boldsymbol{M},\ r,v_y^x)\ Impact(v_y^x)\cdot Weight(x,y)$

7) $r=r+1$ }

8) return ***NSAH***, ***NSAN***

end

在上述算法中 *h* 表示网络中主机总量，*s* 表示服务总数，主机 $host_x$ 包含服务数量为 g_x，$1\leqslant x\leqslant h$，主机 $host_x$ 上的服务 $Service_y$ 在网络所有服务中的重要性权重为 $Weight(x,y)$，$1\leqslant y\leqslant g_x$，该服务上的漏洞 v_y^x 的威胁得分为 $Impact(v_y^x)$，将各轮主机安全态势值保存在矩阵 ***NSAH*** 中，网络安全态势值保存在矩阵 ***NSAN*** 中。

第 1)行表示初始化攻击轮次 $r=0$；令 Prob $(\boldsymbol{M},r,v_y^x)$ 表示矩阵 ***M*** 中，第 *r* 轮攻击利用漏洞 v_y^x 到达状态的发生概率，如第 2)行所示；第 3)行~第 7)行表示求解态势值的递归过程；第 4)行计算服务 $Service_y$ 在主机 $host_x$ 所有服务中的权重；计算第 *r* 轮主机 $host_x$ 的态势值，写入 $NSAH_{r,x}$，如第 5)行所示；计算第 *r* 轮全网态势值，写入 $NSAN_r$，如第 6)行所示。

态势值越大，说明网络系统面临的威胁越严重；反之，网络系统较为安全。通过安全态势量化，将攻击预测得到的低层攻击行为信息映射为定量的网络安全风险值，结合可视化技术可构建多要素、全方位的实时动态演化视图，直观地表达当前网络系统面临的威胁状况及其演化趋势，为安全控制提供参考依据。

5 实验与分析

为了验证本文方法的有效性，搭建了一个类似文献[13]的小型网络环境。实验环境拓扑如图 2 所示，网络中包括防火墙、入侵检测系统、4 台服务

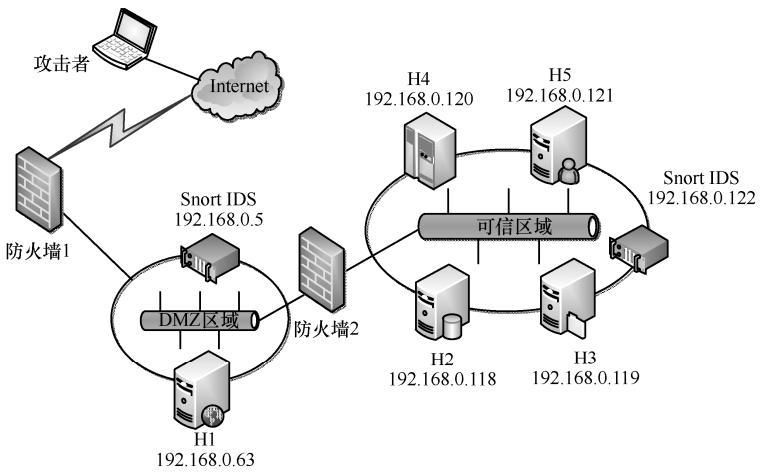


图 2 实验网络拓扑结构

器以及 1 台工作站，防火墙预先设置策略将网络分为 2 个子网。防火墙 1 禁止外部主机访问可信区域中的服务器，外部主机仅可以通过 HTTP 协议(80 端口)与 DMZ 区域中的 Web 服务器进行通信；防火墙 2 允许 DMZ 区域中的服务器和可信区域中的服务器进行通信，且后者仅可以被动接收服务请求。

5.1　网络环境信息

利用脆弱性扫描工具 Nessus 对各网段进行扫描，通过查询 NVD 得到各主机包含的漏洞信息如表 2 所示。考虑主流服务的用户数目多，访问频率大，因此服务重要性更高，通过统计实验过程中的服务访问次数，依据服务访问频率计算不同服务权重。

5.2　测试数据采集

为获取真实的实验数据，从课题依托的实验室中选取网络安全专业学员，在部署环境中进行对抗实验，由外部 Internet 上发起攻击，既定攻击目标为可信区域中认证服务器 H5 的 root 权限。为不影响网络的可用性，对发现漏洞采用修复的基本防御策略，不再考虑变更防火墙策略等其他防御措施。当前情况下所有漏洞的相应厂家均已发布补丁资源，实验检测到该防御者成功修复 1 个漏洞的期望耗时 t=3 h，该时间包括补丁的下载、传输与安装。

根据部署网络的拓扑结构与脆弱性集，利用开源的工具 MulVal 生成网络攻击图，如图 3 所示，图中椭圆表示原子攻击节点，节点转移关系 $\xi=\mathrm{OR}$，边值标注为攻击发生概率。采集网络中运行的防火墙、Snort IDS 和主机安全审计日志处理后的报警信息，利用自动化工具 ArCSight 分析报警数据得到攻击路径，计算各阶段的成功概率。经过检测与对报警数据的处理，发现实际攻击如下。

为获得主机 H5 的 root 权限，攻击者首先对目标网络进行 IPsweep 地址扫描，搜寻有效主机，发生时间为 9:00，发现有效主机 H1，并对其进行端口扫描；发现其通信端口为 80，并利用漏洞 CVE 2014-0098 获得 H1 的 root 权限，发生时间为 9:18，成功概率为 0.73；然后通过 SQL 协议，利用漏洞 CVE 2014-0063 获得服务器 H2 的 root 权限，发生时间为 9:42，成功概率为 0.54；接着利用服务器 H3 的 Linux 内核漏洞获得其 user 权限，发生时间为 10:31，成功概率为 0.35，并利用服务器 H3 的 Microsoft Office 软件漏洞获得其 root 权限，发生时间为 10:50，成功概率为 0.62；随后攻击者利用 BMC 服务漏洞获得工作站 H4 的用户权限，发生时间为 11:36，成功概率为 0.51；以 H4 为跳板，最后利用 radius 服务漏洞达到入侵目的，获得认证服务器 H5 的 root 权限，发生时间为 11:48，成功概率为 0.63。

5.3　计算过程与结果分析

为验证本文研究的有效性，截取 9: 00~10: 00 时间段内的报警数据，利用本文算法分析未来一段时间的攻击行为及安全态势，并与实际捕获数据进行比较。

1) 攻击者能力评估

该时段内攻击者所实施难度最大漏洞的复杂度 AC=Medium，由 3.1 节计算攻击能力 $ACAP$=Medium。

2) 漏洞利用率分析

由表 1 得到攻击者对不同漏洞的实际利用率如表 3 第 2 列所示。

3) 攻击期望耗时量化

结合已发生的针对服务 Apache、postgresql 漏洞的攻击耗时 0.3 h 和 0.4 h，利用 3.3 节方法得到先验平均攻击耗时 $AMTI_{\mathrm{prior}}=0.217\,5$ h，并计算攻击期望耗时如表 3 第 3 列所示。

表 2　网络主机配置及漏洞信息

主机	主机配置	服务名称	CVE #	漏洞描述	*AC*	权重	威胁得分
H1	Web 服务器 Windows Server 2008	Apache	CVE 2014-0098	apache 图形接口 XSS 漏洞	Low	0.1	2.9
H2	Database 服务器 MSQL Server 2003	postgresql	CVE 2014-0063	非认证用户执行任意代码漏洞	Medium	0.2	6.4
H3	FTP 服务器 Red Hat Linux 7.2	Linux	CVE 2013-1324	基于堆栈的缓冲区溢出攻击漏洞	High	0.1	10.0
		MS-office	CVE 2014-0038	指针参数调用超时漏洞	Low	0.1	10.0
H4	图形工作站 Windows XP SP2	BMC	CVE 2013-4782	远程攻击者绕过身份认证执行 IPMI 命令漏洞	High	0.2	10.0
H5	认证服务器 Windows Server 2008	radius	CVE 2014-1878	远程拒绝服务攻击漏洞	Low	0.3	2.9

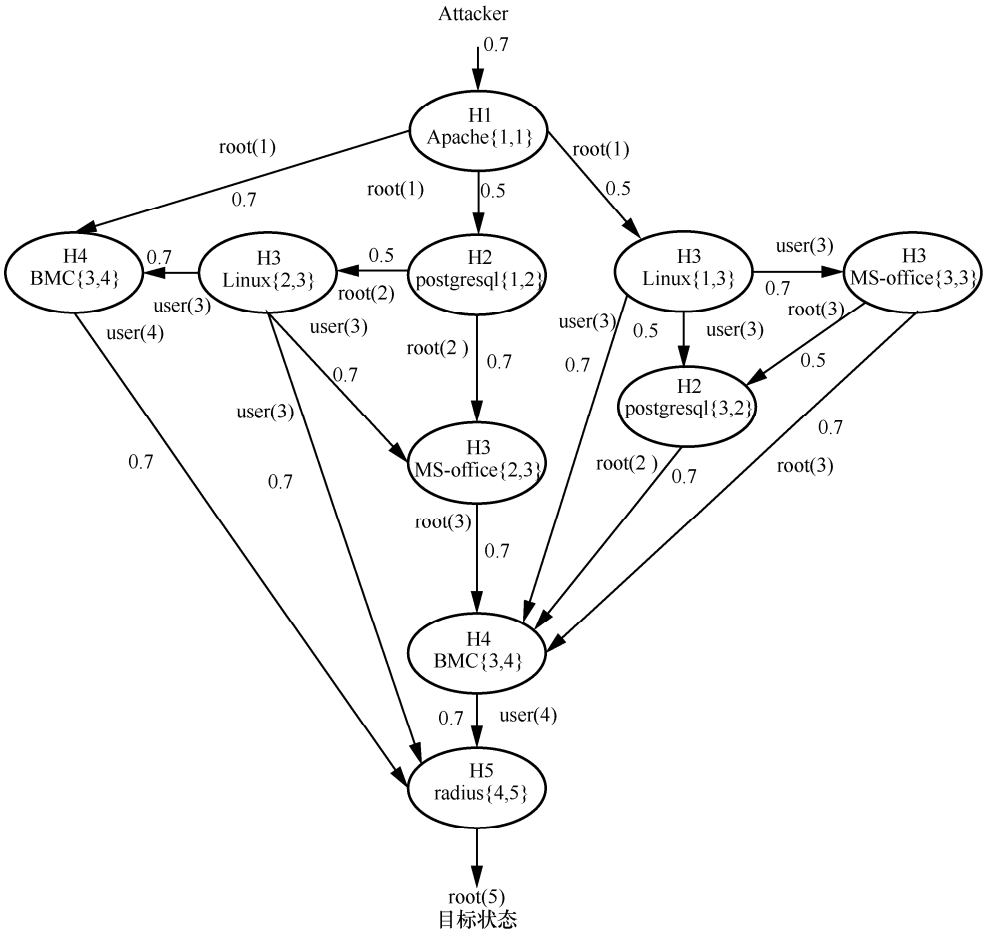


图 3　网络攻击

表 3　　**漏洞利用率与攻击期望耗时**

CVE #	利用率	攻击期望耗时/h
CVE 2014-0098	0.7	0.31
CVE 2014-0063	0.5	0.43
CVE 2013-1324	0.3	0.73
CVE 2014-0038	0.7	0.31
CVE 2013-4782	0.3	0.73
CVE 2014-1878	0.7	0.31

4) 攻击行为预测

由攻击图可知共有 7 种不同的攻击状态，S_1 表示攻击者的初始状态，所有状态信息描述如表 4 所示。根据图 3 和表 3 得到的攻击行为信息如表 5 所示。

由表 5 可知共有 14 种不同的状态转移行为，先验攻击序列 $\mathrm{Path}_{\mathrm{prior}} = S_1 \to S_2 \to S_3$，由定义 4~定义 9 可知，初始状态发生概率向量 $\boldsymbol{P}^0 = \{1, 0.73, 0.54, 0, 0, 0, 0\}$，时间向量 $\boldsymbol{T}^0 = \{0, 0.3, 0.7, 0, 0, 0, 0\}$，结合表 5 构造初始状态转移概率矩阵 ***SP***、攻击期望耗时矩阵 ***AT*** 和防御期望耗时矩阵 ***DT*** 分别为

$$\boldsymbol{SP} = \begin{pmatrix} 1 & 0.73 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0.54 & 0.3 & 0 & 0.3 & 0 \\ 0 & 0 & 1 & 0.3 & 0.7 & 0.3 & 0 \\ 0 & 0 & 0.5 & 1 & 0.7 & 0.3 & 0.7 \\ 0 & 0 & 0.5 & 0 & 1 & 0.3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0.7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\boldsymbol{AT} = \begin{pmatrix} 0 & 0.3 & \infty & \infty & \infty & \infty & \infty \\ \infty & 0 & 0.7 & 0.73 & \infty & 0.73 & \infty \\ \infty & \infty & 0 & 0.73 & 0.31 & 0.73 & \infty \\ \infty & \infty & 0.43 & 0 & 0.31 & 0.73 & 0.31 \\ \infty & \infty & 0.43 & \infty & 0 & 0.73 & \infty \\ \infty & \infty & \infty & \infty & \infty & 0 & 0.31 \\ \infty & \infty & \infty & \infty & \infty & \infty & 0 \end{pmatrix}$$

$$\boldsymbol{DT}=\begin{pmatrix}0&3&0&0&0&0&0\\0&0&3&3&0&3&0\\0&0&0&3&3&3&0\\0&0&3&0&3&3&3\\0&0&3&0&0&3&0\\0&0&0&0&0&0&3\\0&0&0&0&0&0&0\end{pmatrix}$$

表 4　　攻击状态信息

状态编号	状态名称	状态描述
S_1	Initialization	外部用户
S_2	root(1)	(H1, root)
S_3	root(2)	(H2, root)
S_4	user(3)	(H3, user)
S_5	root(3)	(H3, root)
S_6	user(4)	(H4, user)
S_7	root(5)	(H5, root)

表 5　　攻击行为信息

状态转移	CVE #	转移概率	期望耗时/h
$S_1\to S_2$	CVE 2014-0098	0.73	0.3
$S_2\to S_3$	CVE 2014-0063	0.54	0.7
$S_2\to S_4$	CVE 2013-1324	0.3	0.73
$S_2\to S_6$	CVE 2013-4782	0.3	0.73
$S_3\to S_4$	CVE 2013-1324	0.3	0.73
$S_3\to S_5$	CVE 2014-0038	0.7	0.31
$S_3\to S_6$	CVE 2013-4782	0.3	0.73
$S_4\to S_3$	CVE 2014-0063	0.5	0.43
$S_4\to S_5$	CVE 2014-0038	0.7	0.31
$S_4\to S_6$	CVE 2013-4782	0.3	0.73
$S_4\to S_7$	CVE 2014-1878	0.7	0.31
$S_5\to S_3$	CVE 2014-0063	0.5	0.43
$S_5\to S_6$	CVE 2013-4782	0.3	0.73
$S_6\to S_7$	CVE 2014-1878	0.7	0.31

完成参数初始化后，执行算法 1，推演攻击状态转移过程，每执行一次递归，代表一次原子攻击，轮次加 1，终止条件是状态发生概率向量趋于稳定。利用 Matlab 7.1 仿真，算法执行了 4 轮停止，得到各轮攻击过程中的状态发生概率矩阵 $\boldsymbol{M}$ 和时间矩阵 $\boldsymbol{N}$ 分别为

$$\boldsymbol{M}=\begin{pmatrix}1&0.73&0.54&0.381&0.378&0.219&0\\1&0.73&0.54&0.381&0.645&0.447&0.420\\1&0.73&0.54&0.381&0.645&0.527&0.580\\1&0.73&0.54&0.381&0.645&0.527&0.636\end{pmatrix}$$

$$\boldsymbol{N}=\begin{pmatrix}0&0.3&0.7&1.43&1.01&1.43&0\\0&0.3&0.7&1.43&1.74&2.16&1.74\\0&0.3&0.7&1.43&1.74&2.47&2.47\\0&0.3&0.7&1.43&1.74&2.47&2.78\end{pmatrix}$$

算法执行 4 轮停止，因此，整个攻击的路径长度预测值为 $2+4=6$。根据攻击图可知共有 9 条可能的入侵路径如表 6 所示，不同路径的状态转移情况如表 6 所示，攻击步长为 6 的路径包括 Path 4 和 Path 8，通过匹配 $\text{Path}_{\text{prior}}=S_1\to S_2\to S_3$ 可知，攻击者最有可能采取 Path 4 的入侵路径，因此，预测后续状态转移为 $\text{Path}_{\text{posterior}}=S_3\to S_4\to S_5\to S_6\to S_7$。矩阵 $\boldsymbol{M}$ 和 $\boldsymbol{N}$ 的第 4 行分别表示稳定后的状态发生概率和时间向量，得到目标状态 S_7 的成功概率为 0.636，预测攻击者入侵 S_7 的时间为 2.78 h。考虑防御期望耗时 $t=3$ h，因此攻击者在漏洞修复之前可以到达攻击目标，与实际检测结果一致，验证了本文预测算法的有效性。

表 6　　所有攻击路径

路径编号	攻击路径
Path 1	$S_1\to S_2\to S_6\to S_7$
Path 2	$S_1\to S_2\to S_3\to S_4\to S_7$
Path 3	$S_1\to S_2\to S_3\to S_6\to S_7$
Path 4	$S_1\to S_2\to S_3\to S_4\to S_5\to S_6\to S_7$
Path 5	$S_1\to S_2\to S_3\to S_5\to S_6\to S_7$
Path 6	$S_1\to S_2\to S_4\to S_6\to S_7$
Path 7	$S_1\to S_2\to S_4\to S_3\to S_6\to S_7$
Path 8	$S_1\to S_2\to S_4\to S_5\to S_3\to S_6\to S_7$
Path 9	$S_1\to S_2\to S_4\to S_5\to S_6\to S_7$

5) 安全态势量化

结合算法 2，计算主机和网络的安全态势值矩阵，记录在表 7 中，并绘制主机安全态势变化如图 4 所示，横轴为轮次，纵轴为安全态势值，态势值越大表示受到攻击威胁的风险越高。

表 7　　安全态势量化结果 (*t*=3 h)

轮次	主机 H1	主机 H2	主机 H3	主机 H4	主机 H5	全网
0	2.117	3.456	0	0	0	0.903
1	2.117	3.456	3.795	2.190	0	2.105
2	2.117	3.456	5.130	4.470	1.218	3.188
3	2.117	3.456	5.130	5.270	1.682	3.488
4	2.117	3.456	5.130	5.270	1.844	3.536

结合图 4 可以看出，初始阶段主机 H1、H2 处于低风险状态，H3、H4、H5 尚未受到攻击威胁，随着攻击的深入，H3、H4、H5 的安全态势值不断升高，到第 3 轮时前 4 个主机的态势值都趋于稳定，但 H5 的态势值仍趋于升高，说明主机 H5 是最终的攻击目标，通过态势分析可以直观地掌握各主机受威胁的严重程度，为关键资产的安全风险控制提供决策支持。

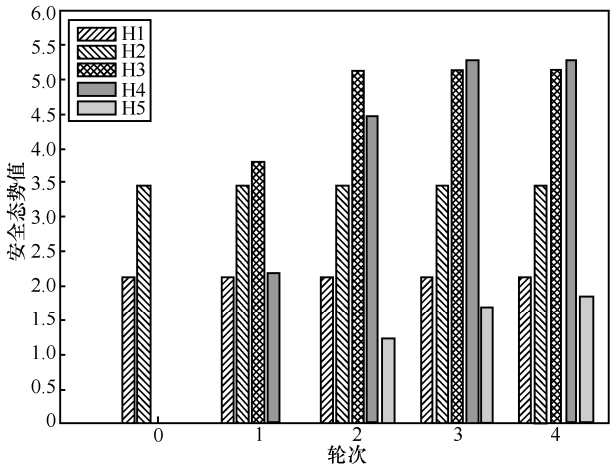


图 4　主机安全态势变化预测（防御期望耗时 *t*=3 h）

为验证防御策略改变对攻击预测和安全态势的影响，通过预先下载漏洞补丁，降低防御期望耗时 $t = 2.5$ h，利用本文方法计算并绘制各主机安全态势变化如图 5。算法执行了 2 轮停止，表示攻击者只执行了 2 步攻击，主机 H5 的态势值为 0，表示未能入侵既定目标。结合 5.2 节实验结果可知，攻击者入侵 H4 的时间为 11:36，此时距离开始攻击过去 2.6 h，在此期间防御者已成功修复主机 H4 上的漏洞，导致攻击无法继续深入，表明本文方法适用于动态防御策略，且验证了所提算法的准确性。

5.4　方案综合对比

以入侵主机 H3、H4 和 H5 的时刻为横坐标，全网态势值为纵坐标，分析本文方法（防御期望耗时 *t*=3 h）、ARIMA 模型[5]、指数平滑法[6]的预测结果与实际测试结果的准确性，对比如图 6 所示，可以看出以下 2 点。

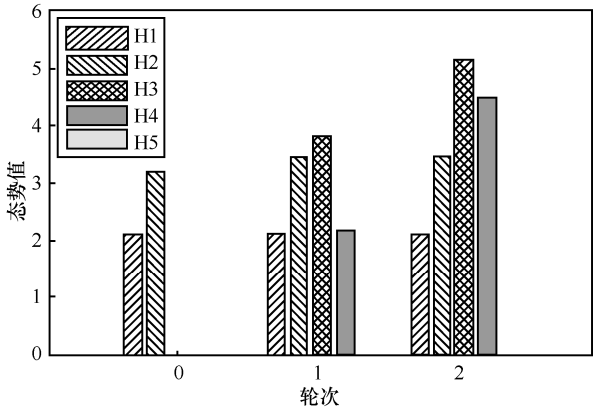


图 5　主机安全态势变化预测（防御期望耗时 *t*=2.5 h）

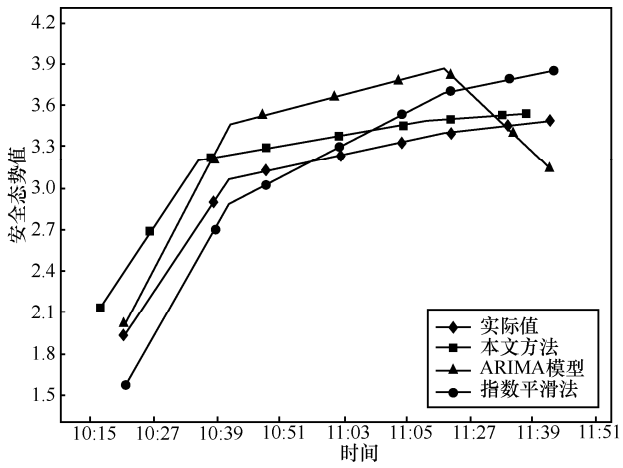


图 6　全网安全态势预测结果对比

1) 在时间预测方面，本文预测攻击各阶段的状态转移耗时与实际值基本一致，随着攻击的深入，不断出现的状态变化可以验证预测的准确性，并作为新的态势要素融入下一轮预测，结果将逐步精确。

2) 在态势预测方面，文献[6]的精度不高，文献[5]中最后阶段的态势值降低，不符合攻击的实际情况，由于实际网络中安全事件突发，而文献[5]中的 ARIMA 模型适用于处理平稳时间序列，因此，预测值可能与实际值违背。本文与实际值更接近，在评估攻击能力时，以其成功利用的最大难度漏洞作为评判标准，不会低估攻击的威胁程度，预测值略高于实际值，利于管理员做好充足的防护控制准备。

本文方法与其他方法的综合比较结果如表 8 所示。

1) 在态势要素构成方面，文献[4, 10, 11]不含防御方信息，文献[3]虽然包含了防御方信息，主要借助安全事件和防护措施的博弈过程确定状态转移矩阵，没有深入分析防御策略变化对风险态势的影响。

表 8　　**本文方法与其他方法综合比较**

算法	态势要素			攻防对抗网络	攻击能力评估	时间预测	算法复杂度
	环境信息	攻击方	防御方				
文献[3]算法	✓	✓	✓	No	Yes	No	$O(n^2)$
文献[4]算法	✓	✓	×	No	No	No	$O(n)$
文献[5]算法	✓	✓	✓	Yes	No	No	$O(n)$
文献[10]算法	✓	✓	×	No	No	No	$O(n^2t)$
文献[11]算法	✓	✓	×	No	No	No	$O(n^2)$
文献[12]算法	✓	✓	✓	Yes	No	No	—
文献[14]算法	✓	✓	✓	Yes	No	Yes	$O(n^2)$
文献[16]算法	✓	✓	✓	Yes	No	No	—
本文算法	✓	✓	✓	Yes	Yes	Yes	$O(mn)$

注：“—”表示文献未提供

2) 在攻击者能力推断方面，本文和文献[3]都对攻击者能力进行了区分与评估，但文献[3]中攻击能力推断是静态的，而本文依据实时观察攻击事件更新攻击能力等级，预测结果更加准确。

3) 在时间预测方面，文献[4, 5, 16]能够识别攻击场景各阶段，但未对时间进行量化，主要分析各时段内网络态势值的变化，本文不仅能量化态势值，且能量化各阶段的具体时间，辅助安全管理员了解入侵速度和节奏。

4) 在算法复杂度方面，本文攻击预测算法的时间复杂度为 $O(mn)$，与文献[3, 10, 11, 14]的算法复杂度阶数相等，虽然略高于其他文献，但符合多项式时间要求，伴随着云存储和并行计算技术的发展，结合分布式处理平台和矩阵分解算法，能够在现有计算能力下实现实时预测。

6　结束语

针对现有研究缺乏对攻击方、防御方与网络环境等态势要素间动态关联，且无法对攻击行为进行多角度、全方位预测的问题，本文提出了一种基于攻击预测的网络安全态势量化方法，本文的主要贡献如下：1) 根据历史攻击行为对攻击者能力进行评估，区分不同的攻击者，并结合漏洞复杂度衡量漏洞的实际利用率；2) 基于采集到的攻击先验耗时计算攻击期望耗时，将攻防耗时融入贝叶斯攻击图，预测后续攻击的发生时间；3) 结合 CVSS 量化标准，从主机和网络 2 个层面度量攻击威胁，给出了一种通用的基于攻击预测的态势量化方法。

本文搭建了一个小型网络模拟攻防实验环境，初步验证了方法的合理性和有效性，为全方位攻击预测和多角度态势量化提供了有效解决思路，并为应用于现实网络环境奠定了理论基础和技术支撑。进一步的工作是尝试采集企业的真实数据集，并结合分布式处理平台，利用云存储和并行计算，优化攻击预测算法中矩阵的存储规模和运算时效性，测试在现实网络对抗环境中的有效性。特别是针对复杂防护策略，如何合理地评估不同防御策略（如防火墙规则变更）的期望耗时、主机安全配置调整对防御耗时度量的影响、量化功能重叠的安全防护设备对防御的贡献权值、提高复杂网络环境中的适用性是未来研究的重点。

参考文献：

[1] QU Z Y, LI Y Y, LI P. A network security situation evaluation method based on D-S evidence theory[C]// Environmental Science and Information Application Technology (ESIAT). 2010:496-499.

[2] 吕慧颖, 彭武, 王瑞梅. 基于时空关联分析的网络实时威胁识别与评估[J]. 计算机研究与发展, 2014, 51(5): 1039-1049.
LYU H Y, PENG W, WANG R M, et al. A real-time network threat recognition and assessment method based on association analysis of time and space[J]. Journal of Computer Research and Development, 2014, 51(5): 1039-1049.

[3] 席荣荣, 云晓春, 张永铮, 等.一种改进的网络安全态势量化评估方法[J]. 计算机学报, 2015, 38(4): 749-758.
XI R R, YUN X C, ZHANG Y Z, et al. An improved quantitative evaluation method for network security[J]. Chinese Journal of Computers, 2015, 38(4): 749-758.

[4] 杨豪璞, 邱辉, 王坤. 面向多步攻击的网络安全态势评估方法[J]. 通信学报, 2017, 38(1): 187-198.
YANG H P, QIU H, WANG K. Network security situation evaluation method for multi-step attack[J]. Journal on Communications, 2017, 38(1): 187-198.

[5] 刘玉岭, 冯登国, 连一峰, 等. 基于时空维度分析的网络安全态势

预测方法[J]. 计算机研究与发展, 2014, 51(8): 1681-1694.
LIU Y L, FENG D G, LIAN Y F, et al. Network situation prediction method based on spatial-time dimension analysis[J]. Journal of Computer Research and Development, 2014, 51(8): 1681-1694.

[6] LING L J, SU L, WANG H F, et al. An ARIMA-ANN hybrid model for time series forecasting[J]. Systems Research And Behavioral Science, 2013, 30(3): 1092-7026.

[7] GE P, WANG J, REN P, et al. A new improved forecasting method integrated fuzzy time series with the exponential smoothing method[J]. International Journal of Environment and Pollution, 2013, 51(3/4): 206-221.

[8] 彭武, 胡昌振, 姚淑萍, 等. 基于时间自动机的入侵意图动态识别方法[J]. 计算机研究与发展, 2011, 48(7): 1288-1297.
PENG W, HU C Z, YAO S P, et al. A dynamic intrusive intention recognition method based on timed automata[J]. Journal of Computer Research and Development, 2011, 48(7): 1288-1297.

[9] 陈小军, 方滨兴, 谭庆丰, 等. 基于概率攻击图的内部攻击意图推断算法研究[J]. 计算机学报, 2014, 37(1): 62-72.
CHEN X J, FANG B X, TAN Q F, et al. Inferring attack intent of malicious insider based on probabilistic attack graph model[J]. Chinese Journal of Computers, 2014, 37(1): 62-72.

[10] LIU S, LIU Y. Network security risk assessment method based on HMM and attack graph model[C]// IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, NETWORKING and Parallel/distributed Computing. 2016:517-522.

[11] FREDJ O B. A realistic graph based alert correlation system[J]. Security & Communication Networks, 2015, 8(15):2477-2493.

[12] DAI F, HU Y, ZHENG K, et al. Exploring risk flow attack graph for security risk assessment[J]. IET Information Security, 2015, 9(6): 344-353.

[13] ABRAHAM S, NAIR S. A predictive framework for cyber security analytics using attack graphs[J]. International Journal of Computer Networks & Communications, 2015, 7(1): 1-17.

[14] GHASEMIGOL M, GHAEMI B A, TAKABI H. A comprehensive approach for network attack forecasting[J]. Computers & Security, 2016,58:83-105.

[15] WANG Y, LI J, MENG K, et al. Modeling and security analysis of enterprise network using attack-defense stochastic game Petri nets[J]. Security & Communication Networks, 2013, 6(1):89-99.

[16] 张勇, 谭小彬, 崔孝林, 等. 基于Markov博弈模型的网络安全态势感知方法[J]. 软件学报, 2011, 22(3): 495-508.
ZHANG Y, TAN X B, CUI X L, et al. Network security situation awareness approach based on Markov game model[J]. Journal of Software, 2011, 22(3): 495-508.

[17] CHEN G, SHEN D, KWAN C, et al. Game theoretic approach to threat prediction and situation awareness[C]//International Conference on Information Fusion. 2006:1-8.

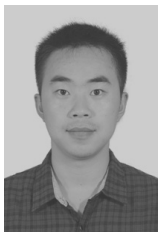
[18] WU J, OTA K, DONG M, et al. Big data analysis based security situational awareness for smart grid[J]. IEEE Transactions on Big Data, 2016, doi:10.1109/TBDATA.2016.2616146.

[19] SERRA E, JAJODIA S, PUGLIESE A, et al. Pareto-optimal adversarial defense of enterprise systems[J]. ACM Transactions on Information & System Security, 2015, 17(3):11.

[20] MELL P, SCARFONE K, ROMAMOSKY S. Common vulnerability scoring system[J]. IEEE Security & Privacy, 2007, 4(6): 85-89.

[21] OU X, GOVINDAVAJHALAS, APPEL A W. MulVAL: a logic-based network security analyzer[C]//14th USENIX Security Symposium. 2005.

作者简介：



胡浩（1989-），男，安徽池州人，解放军信息工程大学博士生，主要研究方向为网络安全态势感知和图像秘密共享。

叶润国（1976-），男，江西萍乡人，博士，中国电子技术标准化研究院工程师，主要研究方向为大数据安全。

张红旗（1962-），男，河北遵化人，博士，解放军信息工程大学教授、博士生导师，主要研究方向为网络安全、风险评估、等级保护和信息安全管理等。

杨英杰（1971-），男，河南郑州人，博士，解放军信息工程大学教授、硕士生导师，主要研究方向为数据挖掘、态势感知和信息安全管理等。

刘玉岭（1983-），男，山东济阳人，博士，中国科学院软件研究所副研究员，主要研究方向为网络安全态势感知。