高技术通讯 2010 年 第 20 卷 第 7 期:680 ~ 684

doi:10.3772/j.issn.1002-0470.2010.07.004

基于因素神经网络理论的网络攻击态势小生境模型研究①

陶 源②*** 刘增良*** 张智南* 王盼卿* 郭春霞*

(*北京科技大学信息工程学院 北京 100083)
(**公安部信息安全等级保护评估中心 北京 100142)
(***国防大学信息作战研究所 北京 100091)

摘 要 结合因素神经网络(FNN)理论,定义了网络攻击态势小生境模型,从攻击角度对目标网络系统整体性能的变化进行了形式化分析。通过攻击态势提取、攻击态势理解和攻击态势显示这三个步骤分别得到了攻击态势因素藤、攻击态势因素网和小生境态势图。最后进行了仿真实验,并给出了网络攻击进行小生境态势图、攻击成功小生境态势图和攻击失败小生境态势图,实验结果表明了该模型可以有效地用于网络攻击仿真研究和仿真训练。

关键词 攻击态势,小生境模型,因素神经网络(FNN),攻击态势因素藤,攻击态势因素网

0 引 言

随着网络的快速发展,网络安全越来越重要[1],同时军事指挥自动化系统在各种恶劣环境下的可信性与可用性,电力调度控制系统的可信性与可用性等,也需要用一定的攻击手段来进行相应的验证。因此,有必要建立一套攻击仿真系统,用于研究网络攻击效果和进行网络攻击仿真训练。而切实有效的态势显示系统是模拟仿真系统的重要组成部分[2,3],网络攻击态势显示系统可以有效地将网络攻击效果显示出来,为其网络攻击效果仿真研究及网络攻击仿真训练提供支持。

目前,国内外学者往往关注于网络态势感知[4,5]和网络防御安全态势[6-8]的研究,无法满足网络攻击仿真研究和网络攻击仿真训练的需求。因此,本文结合因素神经网络(factors neural networke, FNN)[9]理论,建立了网络攻击态势小生境模型,定义了网络攻击的相关因素[10,11],并通过攻击态势提取获得了网络攻击态势因素藤,通过攻击态势理解获得网络攻击态势因素网。在此基础上,结合给定的时间窗口进行分析,可以对网络攻击的总体效果进行相应的攻击态势显示。攻击态势显示提供了直观的网络攻击态势图,便于对网络攻击效果进行宏观的把握和对网络攻击效果的定性评估。同时,也可以根据态势图对网络攻击仿真训练结果进行评判分析,更好地提高网络攻防仿真对抗训练效果。

1 网络攻击态势小生境模型

生境原意为生物和环境,在本文中,将生境定义为网元和网元所处的网络环境,网络攻击态势小生境模型即为可以描述出网络攻击态势的最小网元集合和其所处的最小网络环境。

由于网络攻击的效果不同于目标网络系统某项性能的变化,而是目标网络系统整体性能变化的综合概念。因此,为了便于对目标网络系统整体性能的变化进行定性化描述,本文提出了建立网络攻击态势小生境模型。即网络攻击态势不仅与攻击方的网络环境有关,同时也与攻击目标的网络环境密切相关。

借鉴 FNN 的相关理论,本文定义网络攻击态势小生境模型的 FNN 表达式为

$$\begin{cases} FNN = \langle M, V, D, T, P, \Phi, \Psi, \Theta, W, \tau, \phi, n, \lambda \rangle \\ FN_i = \{ f_i \mid f_i \in FNN \} \\ U = \{ u_i \mid u_i = FN_i \}, \mid U \mid \geqslant 2 \end{cases} \tag{1}$$

在式(1)中, FN_i 是构成网络攻击态势的 FNN 小生境模型的任一因素神经元。而 $W = \{ w_{ij} \mid w_{ij}$ 是由 u_i 到 u_j 权重$\}$,即有 $w: U \times U \to W, (u_i, u_j) \to w_{ij} \in W$。

在网络攻击态势小生境模型中,攻击者为 m_k,

① 国家自然科学基金重大研究计划(90818025),国家自然科学基金(60773127,60173057,60572162)资助项目。
② 男,1981 年生,博士;研究方向:信息安全;联系人,E-mail: taoyuanphd@gmail.com
(收稿日期:2009-04-03)

全体攻击者构成攻击者集合 $M=\{m_1,m_2,\cdots,m_k\}$。攻击方法看作是攻击疫苗 v_j，全体可用攻击方法构成攻击疫苗集合 $V=\{v_1,v_2,\cdots,v_n\}$。攻击者 m_k 的攻击目标定义为 d_k，全体攻击目标为 $D=\{d_1,d_2,\cdots,d_q\}$。攻击者 m_k 完成疫苗攻击 v_j 所需要的时间定义为 $t(v_j)$。攻击者 m_k 在 t 时刻所掌握的目标网络信息定义为 $p_k(t)$。攻击者 m_k 在 t 时刻执行疫苗攻击 v_j 的收益定义为 τ_k。攻击者集合 M 在攻击目标集 D 中获得的所有收益定义为 Φ。攻击者 m_k 在 t 时刻执行疫苗攻击 v_j 的代价定义为 ψ_k，攻击者集合 M 在攻击目标集 D 中付出的所有代价定义为 Ψ。攻击者 m_k 实现攻击目标 D_k 的最大允许代价定义为 $\overline{\Psi}_k$。攻击效用函数为 $n(.)$。时间窗为 λ。

定义网络攻击态势 FNN 小生境模型的初态集为 $\Theta=\{v\mid v\text{ 为任一攻击疫苗}\}\in V$，该模型的运行目标为 $\tau:\Theta\times T\times V\times W\to\Phi,(v,\tau,w)\to\tau\in\Phi$。

因此将攻击者 m_k 在 t 时刻执行疫苗攻击 v_j 的收益 τ_k 定义为

$$\tau_k=\tau_k(v_j,t\mid d_k,p_k(t)) \tag{2}$$

攻击者 m_k 在 t 时刻执行疫苗攻击 v_j 的代价 ψ_k 为

$$\psi_k=\psi_k(v_j,t) \tag{3}$$

将攻击效用函数 $n(.)$ 定义为

$$n(.)=\Phi-\Psi \tag{4}$$

因此，在每个攻击决策时刻 t_m，攻击者 m_k 选取疫苗攻击 v_j 的准则应为

$$\arg\max_{v_j}\{\tau_k(v_j,t_m\mid m_k,p_k(t))\} \tag{5}$$

在实际攻击过程中，攻击者通常会受到各种外界限制条件的制约，因此攻击者实施一次疫苗攻击的代价不仅与完成攻击所需的资源条件有关，同时还与攻击过程被追踪、捕获，并由此受到惩罚的风险有关。无论攻击者是在追求收益最大化的情况下选择代价小的攻击方案，还是不考虑代价，一味追求收益最大化，在本文中，统一定义疫苗攻击的约束条件为

$$\sum_{\forall v_j\in v_j(t_m)}\psi_k(v_j,t)<\overline{\Psi}_k \tag{6}$$

在每一个攻击决策点，攻击者按照式(5)和(6)的要求选择要执行的疫苗攻击。这一疫苗攻击过程一直进行直到达到攻击目的，或者超越了式(6)的约束。

2　网络攻击态势小生境模型分析

为了研究方便，本文将网络攻击态势小生境模型分为攻击态势提取、攻击态势理解和攻击态势显示三个步骤来进行。首先通过攻击态势提取获得网络攻击态势因素藤，再通过攻击态势理解对网络攻击态势因素藤进行融合分析得到网络攻击态势因素网，最后结合时间窗口进行攻击态势显示便得到了网络攻击态势图。

2.1　攻击态势提取

因为攻击事件是由一系列的攻击动作构成的，而一个攻击动作可以是发送一条消息、提交一个任务、执行一段代码等，在本文中将其统一建模为疫苗攻击。而网络攻击的效果体现在目标系统的状态改变，因此为了能够从大量的系统状态信息中提取出有效的攻击态势因素神经元，本文提出网络攻击态势因素藤 Ω 的概念。

定义网络攻击态势因素藤 Ω 为

$$\Omega=\{m_k,v_k,d_k,t_k,\tau_k,\psi_k\} \tag{7}$$

即网络攻击者 m_k 对攻击目标 d_k 采用攻击疫苗 v_j 时所用的攻击时间 t，所获得的攻击收益 τ 以及攻击代价 ψ 便是一条网络攻击态势因素藤。

在式(7)中，攻击目标 $d_k=\{IP,Port,V\}$，其中：$IP=\{IP_1,\cdots,IP_k\}$ 为攻击者 m 掌握的目标 IP 地址集，k 为主机数；$Port_k=\{Port_1,\cdots,Port_n\}$ 为攻击者 m 掌握的主机 IP_k 开放的端口集，n 为主机 IP_k 开放的端口数；$V=\{V_1,\cdots,V_e\}$ 为攻击者 m 掌握的系统漏洞信息，e 为系统漏洞数。

通过获取攻击态势因素藤将涉及到网络攻击的相关小生境模型因素有效地进行提取，便于对目标网络系统的状态进行合适的动态评估。通过攻击态势提取得到网络攻击态势因素藤的流程如图 1 所示。

为了便于进行模型分析，本文定义攻击收益为 $\tau=\{a,x,l\}$，其中 a 为攻击严重度，x 为网元敏感度，l 为弱点相关度。攻击严重度 a 即为对目标网元进行疫苗攻击获得的相关漏洞信息及权限，取决于采用的攻击方法和攻击类型。网元敏感度 x 即为被攻击的个体目标在目标网络系统中的重要性，取决于网元的类型、网元提供的服务以及网元中数据的重要性等因素。弱点相关度 l 为目标主机上漏洞之间的协同作用效果，是因为程序之间的交互增加了攻击的机会，扩大了攻击造成后果的可能性，攻击者可以利用一个软件程序的漏洞(例如某服务程序)作为一个跳板从而利用其他软件程序中的漏洞(例如某应用程序)。

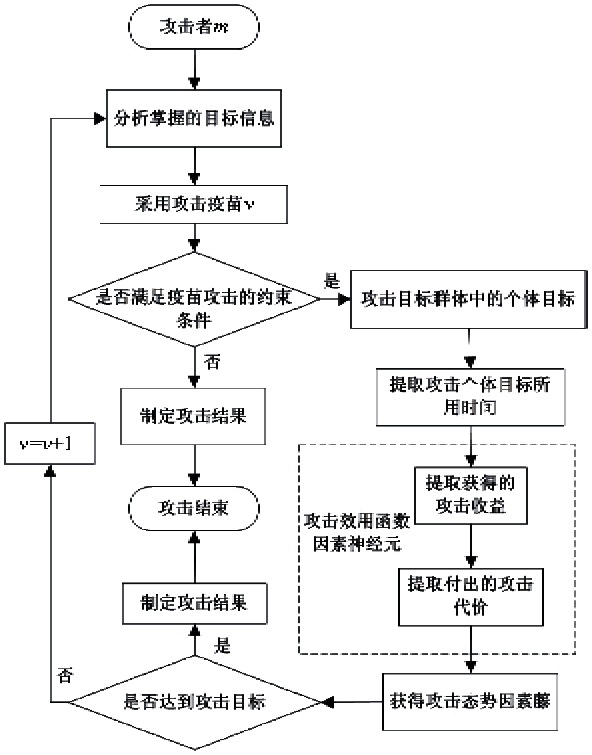

图1 网络攻击态势提取流程图

定义攻击代价 $\psi = \{b, s\}$，其中 b 为资源占用度，s 为攻击风险度。资源占用度 b 是采用某疫苗攻击时所占用网元、带宽等系统资源的一个衡量。攻击风险度 s 是采用某疫苗攻击时被入侵检测系统、防火墙等防御工具发现的几率。

本文采用 DELPHI 法对攻击严重度 a、网元敏感度 x、弱点相关度 l、资源占用度 b 和攻击风险度 s 进行主观赋值，赋值范围为[0,5]，其中5为最高，0为最低。

为了便于进行形式化分析，本文根据攻击对目标网元的攻击结果不同，将攻击态势因素藤 Ω 划分为3个不相交集合，分别为目标网元攻击成功集合、目标网元攻击失败集合、目标网元攻击进行集合，如式

$$\begin{cases} \Omega = \bigcup_{q=1}^{3} \Omega_q \\ \Omega_q = \{\Omega_{i_1}, \Omega_{i_2}, \cdots, \Omega_{i_q}\}, \quad i = 1,2,\cdots,v_m \end{cases} \tag{8}$$

所示。

2.2 攻击态势理解

为了对各个攻击态势因素藤 Ω 的结果进行理解、分析、融合，本文提出了建立攻击态势因素网 Λ 的概念，Λ 即为因素神经藤 Ω 的网络整体性能变化综合结果。在本文中，通过攻击态势理解获得攻击态势因素网 Λ。

定义攻击态势因素网 Λ 如式

$$\Lambda = \omega \circ \Omega = (\eta_1, \eta_2, \cdots, \eta_m) \tag{9}$$

所示。其中，ω 为 Ω 中各因素的归一化模糊权向量，如式

$$\omega = [\widetilde{\omega_1}, \widetilde{\omega_2}, \cdots, \widetilde{\omega_m}] \tag{10}$$

所示。

根据式(8)、(9)、(10)可以得到

$$\Lambda = \begin{bmatrix} \widetilde{\Omega_1} \\ \widetilde{\Omega_2} \\ \cdots \\ \widetilde{\Omega_m} \end{bmatrix} = \begin{bmatrix} \Omega_{11} & \Omega_{12} & \cdots & \Omega_{1n} \\ \Omega_{21} & \Omega_{22} & \cdots & \Omega_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ \Omega_{m1} & \Omega_{m2} & \cdots & \Omega_{mn} \end{bmatrix} \tag{11}$$

其中，Ω_{mj} 表示攻击者 m 对目标网元在采用攻击疫苗 v_j 时的态势因素藤 Ω_{mj}。因此攻击态势因素网 Λ 中的第 m 列 $\eta_m = (\Omega_{m1}, \Omega_{m2}, \cdots, \Omega_{mn})$ 便是攻击者 m 的攻击态势因素藤，它是攻击态势小生境集 FNN 上的模糊子集。

在式(9)中，“$\circ$”是模糊算子，将其定义为 $f(\otimes, \oplus)$，它包含两个操作符“$\otimes$”和“$\oplus$”，其中操作符“$\otimes$”表示乘积运算，操作符“$\oplus$”表示极值运算，因此 η_p 又可以定义为

$$\eta_p = (\omega_1 \otimes \Omega_{1p}) \oplus \cdots \oplus (\omega_n \otimes \Omega_{np}) \tag{12}$$

在式(12)中，$p = 1,2,\cdots,m$。为了结合攻击态势因素藤 Ω 进行形式化分析，本文将模糊算子 $f(\otimes, \oplus)$ 定义为以下三种形式：$f(\vee, \oplus)$，$f(\wedge, \oplus)$ 和 $f(\neg, \oplus)$，各算子的定义如下：

(1)当态势因素藤为目标网元正在被攻击集合时，算子 $f(\wedge, \oplus)$ 是乘积取小算子，即目标网元正在被攻击时取最小的攻击效果，此时的态势为网络攻击进行小生境态势，如式

$$\eta_j = \bigwedge_{i=1}^{m} (\omega_i \wedge \Omega_{ij}) = \min_{1 \leqslant i \leqslant m} \{\omega_i \Omega_{ij}\} \tag{13}$$

所示。

(2)当态势因素藤为目标网元攻击成功集合时，算子 $f(\vee, \oplus)$ 是乘积取大算子，即目标网元攻击成功时取最大的攻击效果，此时的态势为网络攻击成功小生境态势，如式

$$\eta_j = \bigvee_{i=1}^{m} (\omega_i \vee \Omega_{ij}) = \max_{1 \leqslant i \leqslant m} \{\omega_i \Omega_{ij}\} \tag{14}$$

所示。

(3)当态势因素藤为目标网元攻击失败集合时，算子 $f(\neg, \oplus)$ 是乘积有界和算子，即目标网元攻击失败时取其攻击失败的网络边界的攻击效果，此时

的态势为网络攻击失败小生境态势,如式

$$\eta_j = \underset{i=1}{\overset{m}{\neg}}(\omega_i \neg \Omega_{ij}) = \sum_{i=1}^{m} \omega_i \Omega_{ij} / \sum_{i=1}^{m} \omega_i \qquad (15)$$

所示。

例如,1 个 $\Omega = 3$ 的失败攻击,其网络边界的攻击效果为 $(1 \times 3)/1 = 3$,而 3 个 $\Omega = 1$ 的失败攻击,其网络边界的攻击效果为 $(1 \times 1 + 1 \times 1 + 1 \times 1)/(1 + 1 + 1) = 1$,这样可以很好地区分失败的攻击对目标网络边界的整体攻击效果。

在式(13)、(14)和(15)中,$j = 1,2,\cdots,v_n$。

因此,从目标网元的攻击效果角度来将攻击态势因素藤进行归一化模糊融合便得到攻击态势因素网,网络攻击态势理解流程图如图 2 所示。

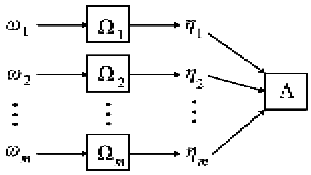

图 2　网络攻击态势理解流程图

2.3　攻击态势显示

为了对攻击态势小生境模型进行整体网络性能变化的综合显示,需要将网络攻击态势因素网 Λ 在给定的时间窗口 λ 中进行分析显示,便得到以 λ 为时间窗口的攻击态势小生境模型的攻击态势图。

定义在给定分析时间窗口 λ 中的网络攻击态势小生境模型的攻击态势为

$$FNN(\lambda) = f(\Lambda(\lambda)) = \sum_{j=1}^{m} \eta_j(\lambda) \qquad (16)$$

这样,攻击态势显示就是将用给定的时间窗口 λ 来对网络攻击态势因素网 Λ 进行分析,具体如图 3所示。为了较好地分析和显示网络攻击态势,时间窗口应该包括较大的时间窗口和较小的时间窗口,这样可以分别提供宏观的和微观的网络攻击态势。

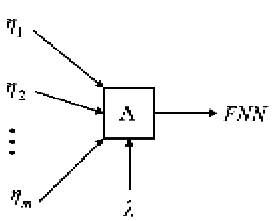

图 3　网络攻击态势显示流程图

综合图 1、图 2 和图 3,便得到了网络攻击态势小生境模型的仿真流程图,如图 4 所示。

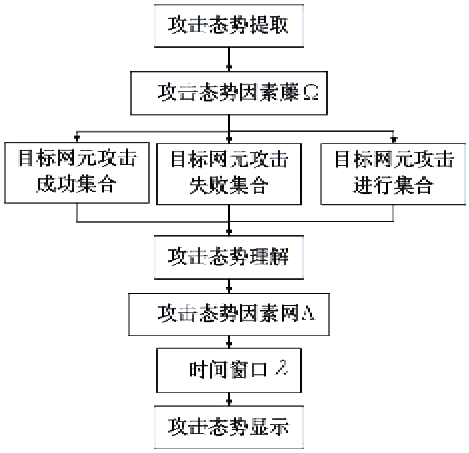

图 4　网络攻击态势小生境模型仿真流程图

3　攻击态势显示实验

根据图 4,本文进行了相应的网络攻击态势小生境模型仿真实验。该仿真实验是在本实验室的群体攻防对抗仿真系统上进行的。在本实验室的群体攻防对抗仿真系统中,攻击目标是 IP 范围为 103.21.45.80 ~ 89 内的主机,其中 IP 为 103.21.45.83 的 WWW 服务器,IP 为 103.21.45.85 的 FTP 服务器,其余为 8 台普通主机,攻击目的是攻破 WWW 服务器和 FTP 服务器。多个攻击方不定期地对该地址段内的网元发起口令猜测、蠕虫、溢出等多种仿真攻击。

在仿真实验中,可以通过选取大小不同的时间窗口获得宏观或微观的小生境态势图,在本文中,无论时间窗口的大小,小生境态势图主要为以下三种:网络攻击进行小生境态势图、网络攻击成功小生境态势图和网络攻击失败小生境态势图。这三种类型的小生境态势图分别如图 5、图 6 和图 7 所示。

图 5　网络攻击进行小生境态势图

在图 5 中,网络攻击进行小生境态势图不断地显示当前正在进行的网络攻击类型和相应的攻击等级,并且给出了当前的攻击时间、攻击目标和攻击源。这为网络攻防仿真和网络攻防仿真训练的宏观监控和总体评价奠定了基础。

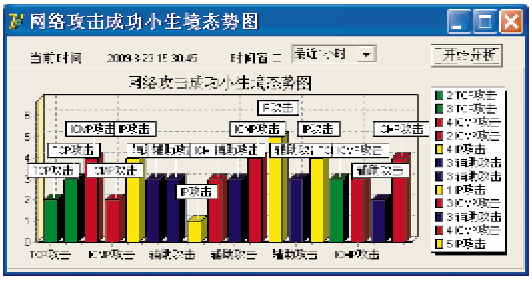

图 6 网络攻击成功小生境态势图

图 7 网络攻击失败小生境态势图

在图 6 中,网络攻击成功小生境态势图将选定的时间窗口内的攻击类型和攻击等级显示出来,为网络攻防仿真和网络攻防仿真训练中研究和评价有效攻击和攻击效用奠定了基础。

在图 7 中,网络攻击失败小生境态势图显示攻击失败的时间和失败的原因,为网络攻防仿真和网络攻防仿真训练中研究和评价攻击代价和攻击疫苗奠定了基础。

4 结 论

本文建立的网络攻击态势小生境模型有效地克服了网络攻击态势的原始数据离散性,在对影响网络攻防态势的各种因素认识模糊、不确定的情况下,可以得到比较合理的网络整体性能变化综合结果,在网络攻防仿真研究和网络攻防仿真训练中具有一定的实用价值。

并且,本文建立的网络攻击态势小生境模型可以通过选取较大或较小的时间窗口,为仿真研究和仿真训练提供宏观或微观的攻击态势图,使研究人员的视野更为集中,便于确定有效攻击、攻击代价等研究内容,也便于仿真训练的总体评价。

参考文献

[1] 沈昌祥,张焕国,冯登国等. 信息安全综述. 中国科学 E 辑:信息科学,2007,37(2):129-150
[2] 马亚明,华一新,张亚军. 战场态势信息数据模型研究. 系统仿真学报,2009,21(4):948-953
[3] Tim B. Intrusion systems and multisensor data fusion: creating cyberspace situation awareness. *Communications of the ACM*, 2000, 43(4): 99-105
[4] Salim H, Guangzhi Q. Impact analysis of faults and attacks in large-scale networks. http://www.ece.arizona.edu:the University of Arizona,2003
[5] Tim B. Cyberspace situational awareness demands mimic traditional command requirements. http://www.silkroad-asia.com:AFCEA Signal Magazine,2000
[6] Julie h. L, Marc G, Luc B, et al. Computer network defence situational awareness. http://pubs.drdc.gc.ca:Technical Memorandum DRDC Ottawa,2005
[7] 赵国生,王慧强,王健. 基于灰色 Verhulst 的网络安全态势感知模型. 哈尔滨工业大学学报,2008, 40(5):798-801
[8] 陈秀真,郑庆华,管晓宏等. 层次化网络安全威胁态势量化评估方法. 软件学报,2006,17(4):885-897
[9] 刘增良,刘有才. 因素神经网络理论及实现策略研究. 北京:北京师范大学出版社,1992.30-42
[10] 鲜明,包卫东,王永杰等. 网络攻击效果评估导论. 长沙:国防科技大学出版社,2007.72-89
[11] 柳亚鑫,吴智发,诸葛建伟. 基于 Vmware 的第三代虚拟 Honeynet 部署以及攻击实例分析. http://www.icst.pku.edu.cn:北京大学计算机科学技术研究所,2005

Research on network attack situation niching model based on FNN theory

Tao Yuan[*,**], Liu Zengliang[***], Zhang zhinan[*], Wang Panqing[*], Guo Chunxia[*]
([*] School of Information Engineer, University of Science and Technology Beijing, Beijing 100083)
([**] MPS Information Classified Security Protection Evaluation Center, Beijing 100142)
([***] Institute of Information Operation, National Defense University, Beijing 100091)

Abstract

The network attack situation niching model is presented by using the factors neural networks theory, so that the overall performance of the target network is analyzed from the attack and formalization angles. The model is carried out by three steps, which are the attack situation extraction, the attack situation comprehension and the attack situation demonstrates. And three return are obtain from these steps, which are the factors rattan of attack situation, the factors net of attack situation and the situation niching map. At last, the simulation experiments are carried on, and three maps are presented, which are the attacks progress situation niching map, the attacks success situation niching map and the attacks failing situation niching map. The results prove that the network attack situation niching model is useful for simulation research and training of network attack.

Key words: attack situation, niching model, factors neural networks (FNN), factors rattan of attack situation, factors net of attack situation