doi:10.11959/j.issn.1000-436x.2016092

基于攻防信号博弈模型的防御策略选取方法

张恒巍，余定坤，韩继红，王晋东，李涛
（信息工程大学三院，河南 郑州 450001）

摘 要：当前基于博弈理论的防御策略选取方法大多采用完全信息或静态博弈模型，为更加符合网络攻防实际，从动态对抗和有限信息的视角对攻防行为进行研究。构建攻防信号博弈模型，对策略量化计算方法进行改进，并提出精炼贝叶斯均衡求解算法。在博弈均衡分析的基础上，设计了最优防御策略选取算法。通过实验验证了模型和算法的有效性，并在分析实验数据的基础上总结了攻防信号博弈的一般性规律，能够指导不同类型防御者的决策。

关键词：动态博弈；不完全信息；攻防信号博弈；精炼贝叶斯均衡；均衡分析；策略选取
中图分类号：TP309 **文献标识码**：A

Defense policies selection method based on attack-defense signaling game model

ZHANG Heng-wei, YU Ding-kun, HAN Ji-hong, WANG Jin-dong, LI Tao
(The Third Institute, Information Engineering University, Zhengzhou 450001, China)

Abstract: Currently defense policies selection based on game theory mostly applied either the complete information game model or the static game model. In order to be more in line with the reality of network attack and defense, attack-defense behavior was studied by dynamic rivalry and incomplete information. The attack-defense signaling game mode was built, the method to quantify policies was improved and an algorithm to obtain the perfect Bayesian equilibrium was proposed. On the basis of analyzing equilibrium, the algorithm for selecting the optimal defense policy was proposed. The simulation experiment demonstrates that the model and algorithms are feasible and effective. By the experimental data, general rules on signaling attack-defense game are summarized, which can guide defenders of different types to make decisions.

Key words: dynamic game, incomplete information, attack-defense signaling game, perfect Bayesian equilibrium, equilibrium analysis, policy selection

1 引言

日趋严重的信息安全事件正不断对网络安全造成巨大危害[1]。为保护网络安全，防火墙、入侵检测和反病毒软件等技术得到广泛应用，但这些技术存在的共同问题是被动等待攻击，只能在攻击发生之后进行检测、发现、应对和补救，而此时往往已造成严重的损失。因此，迫切要求一种新技术，能在攻击发生前对可能的攻击目标、危害、时空特性等进行分析和预测，进而实施主动防御[2]。博弈论是研究各博弈方之间策略对抗、竞争的对策选择理论[3]，网络攻防对抗中所具有的目标对立性、策略依存性和关系非合作性正是博弈论的基本特征[4]，因此，基于攻防博弈模型的网络安全分析和决策方法逐渐成为研究的热点。本文采用信号博弈的框架模型描述攻防之间的矛盾与对抗，解决攻击行为预测

收稿日期：2015-08-01；**修回日期**：2015-10-14
基金项目：国家自然科学基金资助项目（No.61303074, No.61309013）；国家重点基础研究发展计划（“973”计划）基金资助项目（No.2012CB315900）；河南省科技计划基金资助项目（No.12210231003, No.13210231002）
Foundation Items: The National Natural Science Foundation of China (No.61303074, No.61309013), The National Key Basic Research Program of China (973 Program)(No.2012CB315900), Henan Science and Technology Research Project (No.12210231003, No.13210231002)

和最优防御策略选取问题。

在基于博弈模型的网络安全研究中，构建博弈模型时需要面对2个关键问题：博弈信息限制和博弈行动顺序。部分学者采用完全信息和攻防双方同时行动的假设进行建模研究，其中，文献[4]将攻防对抗看成双方拥有完全信息并同时行动的零和博弈过程，构建完全信息静态博弈模型进行防御策略选取方法的研究。文献[5]以网络被攻击后所需要的恢复时间作为收益定义完全信息静态博弈模型，并分析网络安全性。文献[6]运用完全信息博弈理论对网络中发生的攻击行为进行分析，并指导防御策略的选取。为放宽同时行动假设的限制，使模型更加符合网络攻防实际，文献[7]和文献[8]均提出构建攻防随机博弈模型，并在此基础上分别对网络生存性和网络攻击开展研究。而文献[9]则引入动态博弈模型，通过“虚拟节点”将网络攻防图转化为网络博弈树，用于研究主动防御中的策略选择。但是，上述文献均采用了完全信息假设，而这一假设在现实网络攻防中很难满足，降低了研究成果的价值和实用性。为解决攻防博弈中双方信息受限的问题，文献[10]利用不完全信息重复博弈对信息战中参战双方的行为进行建模。文献[11]将不完全信息静态博弈模型运用于蠕虫攻防策略绩效评估，但是未考虑多种防御者类型的情况，且仅对纯策略贝叶斯均衡进行了分析。上述研究都基于同时行动的假设，使用的限制条件依然比较苛刻。

博弈论中的不完全信息动态博弈模型可以同时满足信息受限和非同时行动的条件，对网络攻防博弈的刻画更加贴近实际，其中，经典的信号博弈由于能够描述网络攻防中情报信息对双方决策的关键影响而受到重视。文献[12]运用信号博弈模型，对DDoS攻击的防御机制进行分析，并给出防御策略选取的原则。文献[13]针对信息机密性，运用信号博弈模型对攻防场景进行建模，分析影响攻防双方收益的要素并给出防御建议。但是，上述研究均将攻击者作为信号发送者，防御者被动接收信号，这与实际的网络攻防情形存在偏差，并且均未给出信号博弈的均衡求解方法。在现实社会中，网络安全防御要服从于信息系统的服务定位，由于开放服务的特点以及产品宣传、社会监管和商业利益的需要，防御者采取的防御策略在一定程度上是一种公共知识；另一方面，攻击者在实施攻击之前，可以通过公开或特殊渠道收集信息系统安全防御的等级、主要技术和所使用产品等信息。从网络攻防的一般过程出发，防御者往往是信号发送者，而攻击者是信号接收者，并使用收到的信号对防御者的类型进行分析和判定，进而决定是否攻击、采取何种攻击方式。因此，本文采用防御者为信号发送者，攻击者为信号接收者的结构从动态、不完全信息角度对攻防行为建模，构建网络攻防信号博弈模型，并提出模型的精炼贝叶斯均衡求解方法，基于对均衡策略的分析，实现对最优主动防御策略的选取。

2 网络攻防信号博弈模型及防御策略选取

在网络攻防中，如果防御者能够通过主动作为来影响攻击者的行为，则是一种真正的主动防御方式[14]，而且可能获得更好的防御效果。但是，如何在非完全信息条件和攻防双方动态对抗的情况下，构建攻防行为分析模型，对主动防御方式进行分析和研究是个十分复杂的问题，目前的研究成果极为有限，本文对此进行了尝试和研究。从分析网络攻防过程出发，本文认为防御者主动释放的信息或防御行为被动泄露的各种信息都是攻击者重要的决策依据，这些信息即是防御者发出的信号，防御信号能够影响攻击者的行为，进而改变攻防双方的收益。因此，包含防御信号的防御策略是一种主动防御策略。为此，本文借鉴信号博弈理论，将防御者设为信号发送者，攻击者设为信号接受者，构建攻防信号博弈模型，对攻防双方的动态博弈过程和信号的作用机理进行分析，并研究防御信号对博弈均衡和攻防策略选择的具体影响。

2.1 策略收益量化

攻击者和防御者的策略收益量化是最优防御策略选取的基础，其量化是否合理直接影响防御策略选取结果。姜伟[4]、王元卓[15]等在总结多种攻击防御策略分类的基础上，提出了成本/收益量化方法，但无法对防御者利用信号选择实现伪装自身、欺骗对方的情形进行量化。本文对文献中的策略收益量化方法进行改进，使之适合攻防信号博弈模型。

定义1 系统损失代价（Dcost, damage cost）、攻击致命度（AL, attack lethality）[16]、攻击成本（AC, attack cost）、防御成本（Decost, defense cost）详细定义及相应计算公式见文献[4,15,16]。一般可将防御者的损失Dcost作为攻击者的所得。

定义2 伪装成本（CC, camouflage cost）。伪装是指防御者释放与自身真实防御等级不相符的

信号，用以达到欺骗攻击者的目的。伪装的代价称为伪装成本，通过不同等级防御行动所包含的防御措施的差异之和对伪装成本进行度量。

防御行动是各项防御措施的集合。低等级的防御者要想伪装较高等级，则需要伪装出高等级防御行动中的措施或者这些措施的结果。根据防御措施所防御的攻击行动权限的不同，可将伪装成本分为 3 个级别。

CL1：低等级的防御行动、较高等级的防御行动缺少用于阻止 Probe 权限攻击的防御措施，则防御伪装成本可设为 1~50。

CL2：低等级的防御行动、较高等级的防御行动缺少用于阻止 User 权限攻击的防御措施，则防御伪装成本可设为 50~100。

CL3：低等级的防御行动、较高等级的防御行动缺少用于阻止 Root 权限攻击的防御措施，则防御伪装成本可设为 100~200。

2.2　攻防信号博弈模型定义

目前，基于博弈理论的网络安全防御大多采用完全信息或静态博弈模型，而网络攻防的特点是非合作、不完全信息、动态对抗[17]，完全信息或静态博弈模型无法很好地贴合网络实际。信号博弈是一种不完全信息动态博弈[18]，博弈的局中人分别是信号的发出者和信号的接收者。信号发出者的类型并不为信号接收者所知，但接收者对信号发出者的类型有先验判断。接收者利用信号对发出者的类型做出修正，形成后验判断，进而选择最优行动。本文以信号博弈为基础，构建如下网络攻防信号博弈模型。

定义 3　网络攻防信号博弈模型（ADSGM, attack- defense signaling game model）是一个七元组 $ADSGM=(N,T,M,B,P_A,\overline{P},U)$。

① $N=(N_D,N_A)$是信号博弈的参与者空间。模型中，攻击者 N_A 为信号接收者，防御者 N_D 为信号发送者。

② $T=(T_D, T_A)$是博弈者的类型空间。防御者类型由采取的防御行动所决定，是防御者的私人信息，$T_D=\{t_1, t_2,\cdots, t_n\}$表示防御者类型集合，$T_A=\{t\}$表示攻击者类型集合。

③ M 为防御者的信号空间。$M\neq\varnothing, M=(m_1,m_2,\text{L},m_n)$，信号名称与防御者的类型相对应，防御者可自主选择发送的信号。由于伪装行为的存在，防御者发送的信号和其实际类型不一定完全一致。

④ $B=(D,A)$是行动空间。$D=\{d_1,d_2,\text{L},d_g\}$，$A=\{a_1,a_2,\text{L},a_h\}$表示防御者、攻击者的行动集合，双方的行动策略数均大于 1，即 $g,h\geq 1$。

⑤ P_A 是攻击者的先验信念集合。$P_A\neq\varnothing, P_A=(p_1,p_2,\text{L},p_n)$，表示攻击者对防御者类型 t_j 的初始判断。

⑥ $\overline{P}$ 是攻击者的后验信念集合。后验信念 $\overline{P}(t_j\mid m_l)=(\overline{p}_1,\overline{p}_2,\text{L},\overline{p}_n)$ 为攻击者观察到信号 m_l 后，使用贝叶斯法则调整后对防御者类型 t_j 的判断。

⑦ $U=(U_D,U_A)$是收益函数集合。表示参与者的博弈收益，由所有参与者的策略共同决定。

基于上述定义、文献[4,15]以及本文改进的收益量化方法，可得攻击者在博弈中的收益期望为

$$U_A(m_l,A_i,t_j)=\sum_e Dcost_{ij}(a_e)-AC_{ij} \tag{1}$$

防御者在博弈中的收益期望为

$$U_D(m_l,A_i,t_j)=\sum_e Dcost_{ij}(a_e)-Decost_{ij}-CC \tag{2}$$

其中，A_i 代表攻击策略，t_j 代表防御者类型，a_e 为该攻击策略所包含的原子攻击。

由于同一等级防御策略的投入大致相同，因此，可以认为它们的防御效果基本一致，若某一防御等级下共有 m 个防御策略，则不失一般性地，假设防御者采用等概率 $b_k=\frac{1}{m}$ 选择自身防御等级下的第 k 个防御策略，可以求得防御者在该防御等级下的收益期望

$$U_D(t_j)=\sum_{k=1}^{m} b_k U_{D_k}(m_l,A_i,t_j) \tag{3}$$

2.3　精炼贝叶斯均衡求解

定义 4　攻防信号博弈模型的精炼贝叶斯均衡由策略组合 $(m^*(t),a^*(m))$ 与后验信念 $\overline{P}(t\mid m)$ 组成[18]，并且满足下列条件：

① $a^*(m)\in\arg\max_{a\in A}\sum\overline{p}(t\mid m)U_A(m,a,t)$；

② $m^*(t)\in\arg\max_{m\in M}U_D(m,a^*(m),t)$；

③ $\overline{P}(t\mid m)$ 是攻击者使用贝叶斯法则从先验概率 P_A、观测的信号 m 和攻击者的最优策略 $a^*(m)$ 得到的。

上述定义中，①表示在给定后验信念 $\overline{P}(t\mid m)$ 后，攻击者针对防御者发出的信号所做出的最优行

动；②表示预测到攻击者的最优行动 $a^*(m)$，防御者选择自己的最优防御策略；③是攻击者运用贝叶斯法则得到后验概率的过程。

由于不完全信息动态博弈的均衡求解过程相对静态博弈而言更加复杂。本文首先给出求解攻防信号博弈模型的精炼贝叶斯均衡的过程和步骤描述，然后通过一个例子加以具体演示和说明。

算法过程描述如下。

1) 在攻击者的信息集上建立后验概率推断 $P(t|m)$。

2) 计算攻击者推断依存的最优反应策略集合。

利用 $P(t|m)$ 求子博弈精炼纳什均衡。在博弈的第 2 阶段，攻击者接收到防御者第 1 阶段发送的信号 $m\in M$，在对类型 t_i 的推断为 $P(t|m)$ 的假设下，选择了 $a^*(m)\in A$，最大化自己的期望支付，通过求解

$$\max_{a\in A}\sum p(t|m)U_A(m,a,t)$$

可求得攻击者的最优行动 $a_p^*(m)$。

3) 计算防御者推断依存的最优策略。

在博弈的第 1 阶段，类型为 t_i 的防御者，预期到攻击者的最优反应行动 $a_p^*(m)$，求 $m^*(t)\in M$，最大化自己的支付函数，即求解

$$\max_{m\in M}U_D(m,a_p^*(m),t)$$

得防御者推断依存的最优策略 $m_p^*(t)$。

4) 计算精炼贝叶斯均衡解。

利用 2)、3)得到的参与者推断依存的子博弈精炼纳什均衡 $\{a_p^*(m),m_p^*(t)\}$，求出满足贝叶斯法则的攻击者对防御者类型的推断 $\hat{P}(t|m)$。如果 $P(t|m)$ 与 $\hat{P}(t|m)$ 不冲突，则 $\{a_p^*(m),m_p^*(t),\hat{P}(t|m)\}$ 为网络攻防信号博弈的精炼贝叶斯均衡。

分析上述计算过程可知，设防御者类型为 n，则信息集的数量为 n，求解过程的第 1)步时间复杂度为 $O(n)$；求解过程的第 2)、3)步是子博弈精炼均衡计算，若(防御策略数,攻击策略数)$_{\max}=m$，则由动态博弈基本理论可知[18]，平均时间复杂度均为 $O(m^3)$；求解过程第 4)步的时间复杂度为 $O(n)$。综上，计算精炼贝叶斯均衡解的时间复杂度为 $O(2n+2m^3)$。存储空间消耗集中在策略收益和均衡求解中间值的存储上，空间复杂度为 $O(nm)$。

下面以一个例子具体说明求解过程。在此例中，防御者类型 T_D=(t_1, t_2, t_3)=(高防御等级，中防御等级，低防御等级)，信号与防御者的类型相对应，即为 M_D=(高防御信号，中防御信号，低防御信号)，防御策略空间为其类型与信号的组合，防御者收益为 $U_D(m, a, t)$。攻击者类型 T_A=(t)，行动空间(即其攻击策略)为 A=(A_1, A_2, A_3)，攻击者对防御者类型的先验信念为 P_A，后验信念为 $\hat{P}(t|m)$，收益为 $U_A(m, a, t)$。

设自然 Nature 选择防御者类型，类型 t_1 的概率为 q_1，t_2 的概率为 q_2，t_3 的概率为 q_3。攻击者观察到 m_1 信号后，认为防御者类型{t_1, t_2, t_3}的概率是{o_1, o_2, o_3}；同理，攻击者观察到 m_2, m_3 信号后，认为防御者类型{t_1, t_2, t_3}的概率分别是{p_1, p_2, p_3}、{q_1, q_2, q_3}。(U_A, U_D)表示双方博弈收益，a_{ij} 表示具体的收益值，i=1, 2,…,9，j=1, 2,…,6。网络攻防信号博弈模型如图 1 所示。

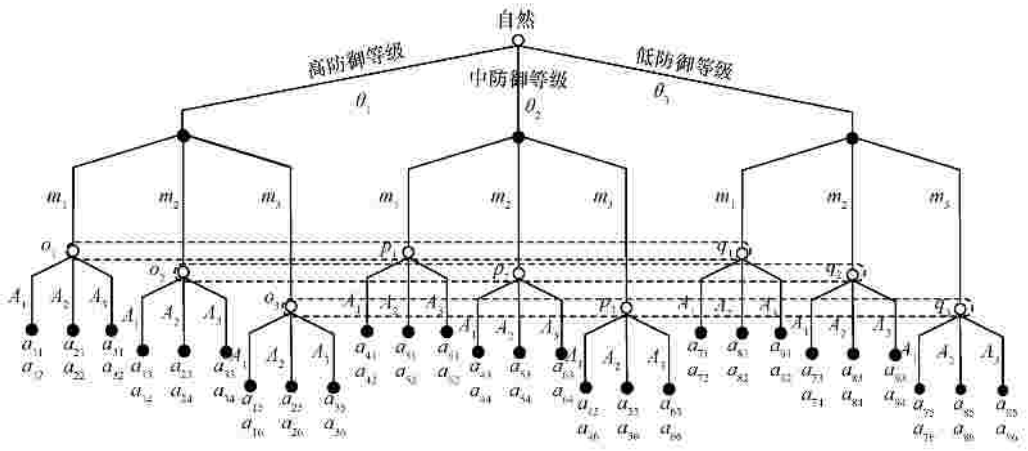

图 1 信号博弈树

按以下步骤来求解网络攻防双方的精炼贝叶斯均衡。

1) 攻击者推断依存的子博弈精炼均衡策略

$$\max_{a\in A}\sum_{t\in T}U_A(m,a,t)p(t\mid m)$$

当 $m=m_1$ 时，

$$\max_{a\in A}\sum_{t_1,t_2,t_3}U_A(m_1,a,t)p(t\mid m_1)$$

$$=\max(U_A(m_1,A_1,t_1)\%(t_1\mid m_1)+U_A(m_1,A_1,t_2)\cdot \%(t_2\mid m_1)+U_A(m_1,A_1,t_3)\%(t_3\mid m_1)$$

$$U_A(m_1,A_2,t_1)\%(t_1\mid m_1)+U_A(m_1,A_2,t_2)\cdot \%(t_2\mid m_1)+U_A(m_1,A_2,t_3)\%(t_3\mid m_1),$$

$$U_A(m_1,A_3,t_1)\%(t_1\mid m_1)+U_A(m_1,A_3,t_2)\cdot \%(t_2\mid m_1)+U_A(m_1,A_3,t_3)\%(t_3\mid m_1))$$

$$=\max\{a_{12}o_1+a_{42}o_2+a_{72}o_3,a_{22}o_1+a_{52}o_2+a_{82}o_3,a_{32}o_1+a_{62}o_2+a_{92}o_3\}$$

由于 $o_1+o_2+o_3=1$，令

$$\begin{cases}a_{12}o_1+a_{42}o_2+a_{72}o_3=a_{22}o_1+a_{52}o_2+a_{82}o_3\\ a_{22}o_1+a_{52}o_2+a_{82}o_3=a_{32}o_1+a_{62}o_2+a_{92}o_3\end{cases}$$

可得

$$o_1^*=\frac{(a_{92}-a_{82})(a_{42}+a_{82}-a_{72}-a_{52})-(a_{82}-a_{72})(a_{52}+a_{92}-a_{82}-a_{62})}{(a_{22}+a_{72}-a_{12}-a_{82})(a_{52}+a_{92}-a_{82}-a_{62})-(a_{32}+a_{82}-a_{22}-a_{92})(a_{42}+a_{82}-a_{72}-a_{52})}$$

$$o_2^*=\frac{(a_{82}-a_{92})(a_{22}+a_{72}-a_{12}-a_{82})-(a_{72}-a_{82})(a_{32}+a_{82}-a_{22}-a_{92})}{(a_{42}+a_{82}-a_{72}-a_{52})(a_{32}+a_{82}-a_{22}-a_{92})-(a_{52}+a_{92}-a_{82}-a_{62})(a_{22}+a_{72}-a_{12}-a_{82})}$$

假设 $o_1^*<o_2^*$，且 $o_1^*,o_2^*\in[0,1]$，则

当 $0<o<o_1^*$ 时，原式 $=a_{12}o_1+a_{42}o_2+a_{72}o_3$，$a(m_1)=A_1$；

当 $o_1^*<o<o_2^*$ 时，原式 $=a_{22}o_1+a_{52}o_2+a_{82}o_3$，$a(m_1)=A_2$；

当 $o_2^*<o<1$ 时，原式 $=a_{32}o_1+a_{62}o_2+a_{92}o_3$，$a(m_1)=A_3$；

同理可求得 p_1^*,p_2^*，当 $0<p<p_1^*$ 时，$a(m_2)=A_1$；当 $p_1^*<p<p_2^*$ 时，$a(m_2)=A_2$；当 $p_2^*<p<1$ 时，$a(m_2)=A_3$。

同理可求得 q_1^*,q_2^*，当 $0<q<q_1^*$ 时，$a(m_3)=A_1$；当 $q_1^*<q<q_2^*$ 时，$a(m_3)=A_2$；当 $q_2^*<q<1$ 时，$a(m_3)=A_3$。

2) 防御者推断的子博弈精炼均衡策略

$$\max_{m\in M}U_D(m,a(m),t)$$

当 $t=t_1$ 时，

$$\max_{m\in M}U_D(m,a(m),t_1)$$

当 $0<o<o_1^*$，$0<p<p_1^*$，$0<q<q_1^*$ 时，原式 $=\max\{U_D(m_1,a(m_1),t_1),U_D(m_2,a(m_2),t_1),U_D(m_3,a(m_3),t_1)\}=\max\{a_{11},a_{23},a_{35}\}$，由此可得 $m(t_1)$。

同理，可得 $0<o<o_1^*$，$p_1^*<p<p_2^*$，$0<q<q_1^*$ 情况下的 $m(t_1)$。

同理，可得 t_2、t_3 类型的子博弈精炼均衡策略。

3) 求解信号博弈的精炼贝叶斯均衡

已知 $m^*(t)$，$a^*(m)$，求出满足贝叶斯法则的攻击者对防御者类型的推断 $\%^*=\%(t\mid m)$，如果 $P(t\mid m)$ 与 $\%(t\mid m)$ 不冲突，即可得出信号博弈的精炼贝叶斯均衡策略 $\{m^*(t),\ a^*(m),\ \%^*\}$。

依据博弈理论，精炼贝叶斯纳什均衡下的混合策略是双方的最优选择 [18]。因此，在此均衡下的防御策略具有最佳效果，防御方应将其作为最优防御策略。

2.4 最优防御策略选取算法及对比分析

基于上述研究，给出基于攻防信号博弈模型的防御策略选取算法的具体表述。

输入：信号攻防博弈树

输出：最优防御策略

开始

1) 初始化 $ADSGM=(N,T,M,B,P_A,\%,U)$；

2) 构建防御者类型空间集合 $T_1=\{t_i,1\le i\le n\}$；

3) 构建防御者信号空间集合 $M=\{m_l,1\le l\le n\}$；

4) 构建防御行动集合 $D=\{d_j,1\le j\le m\}$；

5) 对防御者类型 $t_i\in T_1$ 及信号 $m_l\in M$，有 $d_i\in D$，$U_D(m_l,d_i,t_j)=\sum_e Dcost_{ij}(a_e)+Decost_{ij}+CC$；

6) 对攻击行动，有 $U_A(m_l,d_i,t_j)=\sum_e Dcost_{ij}(a_e)+AC_{ij}$；

7) 建立先验概率推断 $P(t\mid m)$；

8) 攻击者最优反应行动 $a_p^*(m)=\arg\max_{a\in A}\sum_{t\in T}U_A(m,a,t)p(t\mid m)$；

9) 防御者推断的最优策略 $m_p^*(t)=\arg\max_{m\in M}U_D(m, a(m),t)$ ；

10) 求出满足贝叶斯法则的防御者类型的后验概率推断 $\hat{P}(t\mid m)$ ；

11) if $P(t\mid m)$ 与 $\hat{P}(t\mid m)$ 不冲突；

12) then 求得精炼贝叶斯均衡{ $d_p^*(m)$, $m_p^*(t)$, $\hat{P}(t\mid m)$ }；

13) return $m_p^*(t)$ ；

结束

该算法的时间复杂度主要集中在精炼贝叶斯均衡解的计算部分，根据 2.3 节的分析可得，算法的时间复杂度为 $O(2n+2m^3)$ ；算法的空间消耗集中在存储收益计算和均衡求解的中间结果，时间复杂度为 $O(nm)$ 。

将本文的方法和其他文献的方法进行比较，结果如表 1 所示。一方面，信号博弈作为不完全信息博弈模型，与完全信息博弈相比，其考虑了攻防双方不清楚对方信息的情况，更加贴近攻防实际情形；另一方面，静态博弈要求攻击者和防御者同时做出选择，而信号博弈作为动态博弈模型，充分考虑了攻防双方行动的非同时性，更加符合实际要求。

模型的通用性是指模型中的类型集合和策略集合是否可以扩展至 n。若可以，说明模型的通用性较好；若不可以，则说明该模型仅适用于特殊情况，推广应用性较差。均衡求解是指文中是否给出博弈均衡的求解过程，与静态博弈相比，动态博弈的均衡动态变化，求解过程更加复杂，而文献[13]未给出均衡求解方法，文献[12]的方法过于简略，可重复性差。

若将信号博弈中防御者的信号忽略，则此博弈可以看作是不完全信息静态博弈。不完全信息静态博弈模型中攻击者对防御者类型的判断是基于历史数据做出的先验概率，是预设且不可更改的，与实际的博弈场景并不吻合，影响博弈分析的准确性。与之相比，网络攻防信号博弈模型假设攻击者采用后验概率修正防御者类型判断，符合攻防过程中攻击者利用已有信息动态修正自身判断的实际。在网络攻防中，防御者主动释放的信息或其行为透露的各种信息，是攻击者进行决策的重要依据。因此，信号的作用是普遍存在的，并具有重要的关键影响，若在博弈过程中忽略信号，则分析结论将会偏离实际。同时，防御者精心选择信号后再进行释放，能够形成主动防御能力，提升防御效能和主动性。

3 仿真实验与分析

3.1 仿真实验环境描述

为验证所提出的网络攻防信号博弈模型及相关均衡求解方法，部署如图 2 所示的网络信息系统

表 1 不同方法比较结果

方法	信息需求	博弈类型	博弈者类型	发送信号	模型通用性	均衡求解	具体应用
文献[4]	完全信息	静态	1	—	差	简单	策略选取
文献[11]	不完全信息	静态	2	—	差	详细	效能评估
文献[12]	不完全信息	动态	3	攻击者	一般	简单	机制分析
文献[13]	不完全信息	动态	3	攻击者	一般	无	—
本文	不完全信息	动态	n	防御者	较好	详细	策略选取

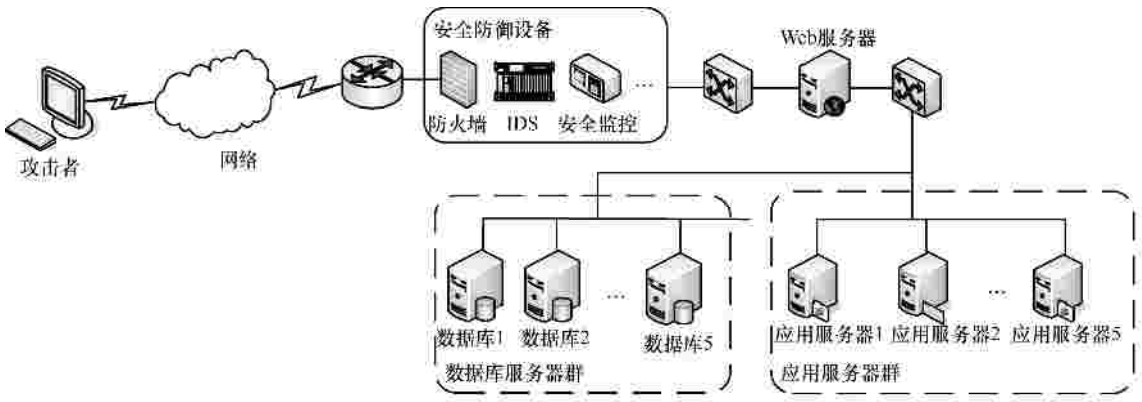

图 2 实验信息系统结构示意

进行仿真实验。该系统主要由安全防御设备、Web 服务器、应用服务器和数据库服务器组成。访问控制规则规定非本网络的主机只能访问 Web 服务器，系统内 Web 服务器、应用服务器可以对数据库服务器进行访问。

假设攻击者仅有权限访问 Web 服务器，无法直接访问应用服务器和数据库。但是，由于系统的漏洞间存在相互依赖关系，攻击者可以通过一系列的原子攻击来获得访问应用服务器和数据库的权限[19]。文献[20]给出攻击者的原子攻击信息如表 2 所示。

表 2　　原子攻击描述

原子攻击名称	分类	*AL*
a_1:remote buffer overflow	Root	10
a_2:install Trojan	Probe	3
a_3:steal account and crack it	User	5
a_4: send abnormal data to GIOP	Root	10
a_5: LPC to LSASS process	Probe	4
a_6:shutdown database server	Root	10
a_7: Oracle TNS listener	Root	10
a_8: Ftp rhost attack	User	5
a_9:Sr-Hard blood	Root	10

3.2　博弈收益计算

利用文献[4,16]给出的方法对输入的路由器配置文件、漏洞数据、防火墙和防御策略进行建模和分析，可得到攻击者可能采用的攻击策略 $A_1\{a_1, a_4, a_8\}$、$A_2\{a_2, a_6, a_7\}$和 $A_3\{a_3, a_5, a_9\}$，根据历史数据，可得其操作代价 *AC* 分别为- 610、- 405、- 325。防御者选取的防御行动常常是各项防御措施的集合，不同类型的防御者选取的行动是不相同的。为简洁有效地说明问题，实例中将防御者分为高防御等级和低防御等级 2 类，信号有高防御信号和低防御信号。参考 MIT 林肯实验室攻防分类[21]，从防御行为库选出可用的防御行动后，经过对成本、影响及专家建议等方面的考虑，不同类型可供选取的防御行动如表 3 所示。其中，各防御行动的操作代价、负面代价和残余系数如表 4 所示。

设定防御措施伪装成本(*CL*1, *CL*2 ,*CL*3)=(10, 50, 100)，安全属性代价的高、中、低分别用 30、20、10 来表示。其中，Web 服务器和应用服务器的安全属性代价为 20，数据库服务器的安全属性代价为 30，P_i=P_c=0，P_v=1。Web 服务器和应用服务器的 Criticality 为 4，而数据库服务器的 Criticality 为 5。防御者的类型为高等级时选择防御策略 (d_1, d_2, d_3, d_4)，低等级时选择防御策略 $(d_5, d_6,$

表 3　　不同类型防御者行动

防御原子策略	防御者							
	高防御等级				低防御等级			
	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8
limit packets from ports	v	v		v	v		v	
install Oracle patches	v	v	v	v			v	v
reinstall listener program	v		v				v	v
uninstall delete Trojan		v		v				
limit access to MDSYS.SDO_CS		v		v		v	v	v
renew data(root)	v		v	v	v			
restart database server	v	v			v	v		
limit SYN/ICMP packets		v	v	v			v	v
add physical resource	v					v	v	
repair database	v	v	v		v	v	v	
correct homepage			v	v				v
delete suspicious account	v	v	v	v			v	
redeploy firewall rule and filtrate malicious packets		v		v		v	v	
address blacklist	v		v		v	v		v
patch SSH on Ftp sever			v		v			v

d_7, d_8），策略选择概率均为 $(0.25, 0.25, 0.25, 0.25)$。攻击者对防御者类型的先验信念 $(q_1, q_2)=(q, 1-q)=(0.4,\ 0.6)$。

表 4 防御行动描述

名称	*Ocost*	*Ncost*	*Rcost* 中 e 的取值
d_1	60	200	$e_2=e_5=e_6=e_7=e_8=1, e_1=e_3=e_4=e_9=0$
d_2	70	240	$e_1=e_4=e_5=e_8=1, e_2=e_3=e_6=e_7=e_9=0$
d_3	10	50	$e_1=e_2=e_3=e_4=e_6=e_8=e_9=1, e_5=e_7=0$
d_4	10	60	$e_1=e_3=e_4=e_5=e_6=e_7=1, e_2=e_8=e_9=0$
d_5	30	80	$e_1=e_3=e_4=e_5=e_7=1, e_2=e_6=e_8=e_9=0$
d_6	25	110	$e_1=e_3=e_4=1, e_2=e_5=e_6=e_7=e_8=e_9=0$
d_7	75	180	$e_1=e_2=e_5=e_6=e_7=1, e_3=e_4=e_8=e_9=0$
d_8	65	260	$e_1=e_2=e_8=1, e_3=e_4=e_5=e_6=e_7=e_9=0$

为提高仿真实验以及分析的针对性和直观性，考察攻防博弈时系统的性能变化情况。文献[22]中对 QoS 性能的分析方法，采用使用频率最高的 Web 浏览、Ftp 下载和在线视频 3 种服务，通过服务平均延迟率（SDP, service delay percent）量化考察实施不同防御策略时，系统的性能损失。实验中在不同博弈场景下对上述 3 种服务分别完成 10 次，取平均完成时间，与无攻击时的平均完成时间进行对比，获得服务平均延迟率，具体数值如图 3 所示。

通过文献[4,15]中的公式及本文式(1)和式(2)计算攻击者和防御者的策略收益。当防御者类型为高防御等级 t_1（采用行动 d_1），发出 m_1 信号，攻击者采取攻击行动 A_1 时：

$$U_A=\sum Dcost_{ij}(a_e)-AC_{ij}=10\times4\times20+10\times5\times30-710=1590$$；

$$U_D(t_1,d_1)=\sum Dcost_{ij}(a_e)-Decost_{ij}-CC=10\times4\times20+10\times5\times30-210=2090$$。

同理可得，当防御者采用行动 d_2、d_3、d_4，则 $U_D(t_1,d_2)=2105$，$U_D(t_1,d_3)=1830$，$U_D(t_1,d_4)=2255$，$U_A=1590$。综上，当防御者类型为高防御等级，发出 m_1 信号，攻击者采取攻击行动 A_1 时，$U_A=1590$，$U_D=0.25(2090+2105+1830+2255)=2070$。

通过上述过程可求得其余策略收益值，形成的博弈树如图 3 所示。

3.3 均衡求解和防御策略选择

经过分析，可得 $p^*=0.68, q^*=0.22$。

1) 防御者类型为高防御等级 t_1

当 $p>p^*, q>q^*$ 时，$a_p^*(m_1)=A_1$，$a_p^*(m_2)=A_3$，$m_p^*(t)=m_1$；

当 $p>p^*, q<q^*$ 时，$a_p^*(m_1)=A_2$，$a_p^*(m_2)=A_3$，$m_p^*(t)=m_1$；

当 $p<p^*, q>q^*$ 时，$a_p^*(m_1)=A_1$，$a_p^*(m_2)=A_2$，$m_p^*(t)=m_1$；

当 $p<p^*, q<q^*$ 时，$a_p^*(m_1)=A_1$，$a_p^*(m_2)=A_1$，$m_p^*(t)=m_2$。

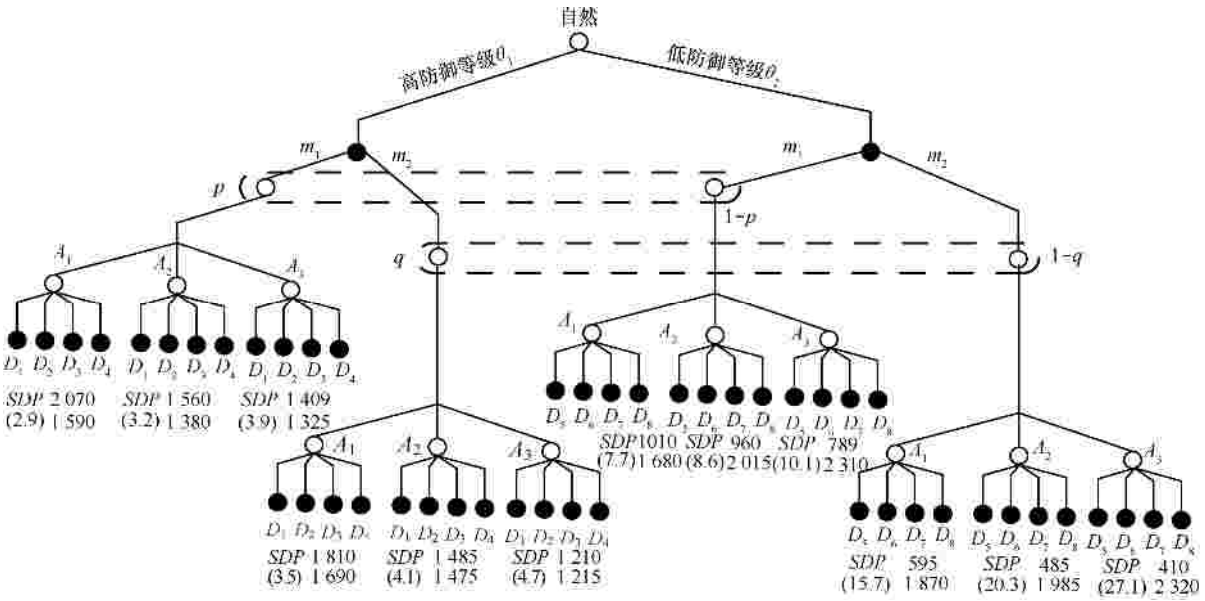

图 3 网络攻防信号博弈树

2) 防御者类型为低防御等级 t_2

当 $p > p^*, q > q^*$ 时，$a_p^*(m_1) = A_1$，$a_p^*(m_2) = A_3$，$m_p^*(t) = m_1$；

当 $p > p^*, q < q^*$ 时，$a_p^*(m_1) = A_1$，$a_p^*(m_2) = A_3$，$m_p^*(t) = m_1$；

当 $p < p^*, q > q^*$ 时，$a_p^*(m_1) = A_2$，$a_p^*(m_2) = A_3$，$m_p^*(t) = m_2$；

当 $p < p^*, q < q^*$ 时，$a_p^*(m_1) = A_2$，$a_p^*(m_2) = A_2$，$m_p^*(t) = m_2$。

由此可得到网络攻防信号博弈模型的精炼贝叶斯均衡的情况如下。

当 $p > p^*, q > q^*$ 时，防御者采用类型为高防御等级 t_1，发出高防御信号 m_1，攻击者采用攻击策略 A_1；防御者采用类型为低防御等级 t_2，发出高防御信号 m_1，攻击者采用攻击策略 A_1。此时为混同均衡，精炼贝叶斯均衡为 $[(m_1, m_1) \to (A_1, A_1), p = q, q > q^*]$，记为 PE1。

同理，

当 $p > p^*, q < q^*$ 时，精炼贝叶斯均衡为 $[(m_1, m_1) \to (A_2, A_1), p = q, q > q^*]$，为混同均衡，记为 PE2。

当 $p < p^*, q > q^*$ 时，精炼贝叶斯均衡为 $[(m_1, m_2) \to (A_1, A_3), p = 1, q = 0]$，为分离均衡，记为 PE3。

当 $p < p^*, q < q^*$ 时，精炼贝叶斯均衡为 $[(m_2, m_2) \to (A_1, A_2), p = q, q > q^*]$，为混同均衡，记为 PE4。

由于 (q_1, q_2)=(0.4, 0.6)，$q_1 < p^*, q_2 > q^*$，所以此时的精炼贝叶斯均衡为 PE3：[(m_1, m_2) ? (A_1, A_3), p=1, q=0]。在此均衡下，当防御者采用高防御等级 t_1，发出高防御信号 m_1，攻击者采用攻击策略 A_1，防御者收益为 2 070，服务平均延迟率为 2.9%；当防御者采用低防御等级 t_2，发出低防御信号 m_2 时，攻击者采用攻击策略 A_3，防御者收益为 410，服务平均延迟率为 27.1%。表明防御者采用高防御等级的防御行动，同时释放高防御信号，是最优防御策略。这种情况说明防御者利用信号的作用表明自己的防御能力，对攻击者产生威慑作用，起到阻止或削弱攻击危害的效果，在一定程度上达到了“不战而屈人之兵”的目的，发挥了主动防御的优势。

3.4 实验分析

仿真实验采用 Matlab 2012 实现了防御策略选择算法，算法运行时间为 2.6 s。实验中的攻击策略操作代价代表实施某一攻击策略所耗费的系统资源和时间，采用 CVSS 数据库[23]中的系统漏洞可获取性（AV）、攻击复杂度（AC）、可利用性（AU）参数进行量化；安全属性代价表示攻击造成系统的完整性、机密性和可用性等安全属性的损失，具体计算方法见文献[4,15]；防御伪装成本代表防御者通过主动行为隐藏自身真实等级，欺骗攻击者所耗费的代价，主要是释放虚假信号的成本；攻击者和防御者策略收益是计算博弈均衡的基础，在实验中是对攻防双方付出代价和获得回报的综合性量化描述。

在不考虑 ?、p、q 具体值的情况下，通过对攻防信号博弈模型的均衡和数据进行一般性分析，可以得到以下规律。

1) 低等级防御者进行伪装可以提高防御效能。图 3 中，低等级防御者 t_2 释放低防御信号 m_2 时的可能收益分别是(595，485，410)，服务平均延迟率为(15.7，20.3，27.1)；释放高防御信号 m_1 时的可能收益分别是(1 010，960，789)，服务平均延迟率为(7.7，8.6，10.1)。说明低等级防御者进行伪装后，通过释放虚假信号起到了混淆、欺骗、迷惑攻击者的作用，使攻击者对其防御等级的判断出现偏差，从而降低攻击概率或影响攻击行为选择，可以使自己的收益期望增大，提高了防御效能。在攻防对抗和作战理论上这是一种“不能而示之能”的主动防御策略，可以在自身防御能力弱小时获取超出能力的防御效果。

2) 遭受攻击时，高等级防御者的收益大于低等级防御者，即高等级防御者的期望损失较小。图 3 中，高等级防御者的可能收益分别是(2 070，1 560，1 409，1 810，1 485，1 210)，服务平均延迟率为(2.9，3.2，3.9，3.5，4.1，4.7)；低等级防御者的可能收益分别是(1 010，960，789，595，485，410)，服务平均延迟率 SDP 为(7.7，8.6，10.1，15.7，20.3，27.1)。由于高等级防御者对安全防御投入多，对网络攻击具有较高的防御能力；而低等级防御者的投入少，防御能力低，当受到攻击时，损失会比较大的。因此，在条件具备时保障安全防御投入，未雨绸缪地增强网络防御能力是避免重大安全风险

和损失的关键，也是最优选择。

3) 高等级防御者应完善信号释放机制，争取分离均衡。图 3 中，在分离均衡下高等级防御者释放高防御信号，可能收益为(2 070，1 560，1 409)，服务平均延迟率 *SDP* 为(2.9，3.2，3.9)；反之，如果高等级防御者释放低防御信号，可能收益为(1 810，1 485，1 210)，服务平均延迟率 *SDP* 为(3.5，4.1，4.7)。在分离均衡下，不同等级防御者选择不同的信号，信号起到标识防御者等级的作用，攻击者可以通过信号对防御者类型进行判断。高等级防御者可以利用信号宣示自己的防御能力水平，威慑、阻止、降低攻击发生概率，提升防御效能，故分离均衡对其比较有利。因此，高等级防御者应积极改进自身的信号释放机制，采取公信力和说服力强的方式释放信号，例如争取由权威的国际性组织或政府部门等可信第三方在公开网络上出具信息安全防护等级评测证书等资质性、认定性文件。

4) 低等级防御者可使用主动释放“虚假”信号作为应急防御手段。由 1)可知，低等级防御者进行伪装，释放虚假信号可以提高防御效能。因此，对低等级防御者而言应小心隐藏有关自身防御能力水平的信息，同时可以在不违反法律的前提下，在公开网络上主动展示一定的“虚假”信息，欺骗攻击者来保护自己。但是，只能作为应急性非常规手段，因为必须承担法律风险；同时，一旦伪装被识破，不但可能遭受严重攻击，而且会严重损害信誉度，造成长期损失。

4 结束语

传统的网络安全技术已无法很好地应对日益严重的网络威胁。为此，本文提出了网络攻防信号博弈模型，根据防御者角色的不同将其划分为多种类型，将防御者释放信号与攻击者进行博弈的过程形式化建模。

由于攻防策略收益量化结果直接影响分析结论，本文对策略收益量化方法进行改进，使其适用于网络攻防信号博弈模型。在此基础上，提出精炼贝叶斯均衡求解方法，并以此为依据选取最优主动防御策略。通过一个仿真实例对提出的模型和方法的有效性进行了验证。研究成果为不完全信息条件下的攻防对抗研究提供了有效的模型方法，并能够对主动防御策略的选取提供指导。

参考文献：

[1] LIANG X N, YANG X. Game theory for network security[J]. Communications Surveys & Tutorials, 2014, 15(1): 472- 486

[2] ZONOUZ S A, KHURANA H, SANDERS W H. RRE: a game- theoretic intrusion response and recovery engine[J]. Parallel and Distributed Systems, 2014, 25(2): 395-406.

[3] FALLAH M S. A puzzle-based defense strategy against flooding attacks using game theory[J]. Dependable and Secure Computing, 2013, 67(1): 5-19.

[4] 姜伟, 方滨兴, 田志宏. 基于攻防随机博弈模型的防御策略选取研究[J].计算机研究与发展,2013,47(10):1714-1723.
JIANG W, FANG B X, TIAN Z H. Research on defense strategies selection based on attack-defense stochastic game model[J]. Journal of Computer Research and Development, 2013, 47(10): 1714-1723.

[5] LYE K, WING J. Game strategies in network security[J]. International Journal of Information Security, 2015, 54(1/2):71-82.

[6] WHITE J, PARK J S, KAMHOUA C A, et al. Game theoretic attack analysis in online social network (OSN) services [C]//The 2014 International Conference on Social Networks Technology. Los Angeles, c2014: 1012-1019.

[7] WANG C L, MIAO Q, DAI Y Q. Network survivability analysis based on stochastic game model[J]. Multimedia Information Networking and Security, 2014, 55(10): 199 -204.

[8] YU M, LIU C, QIU X L, et al. Modelling and analysis of phishing attack using stochastic game[J]. Cyberspace Technology, 2013, 46(3): 300-305.

[9] 林旺群, 王慧, 刘家红. 基于非合作动态博弈的网络安全主动防御技术研究[J].计算机研究与发展, 2013, 48(2): 306-316.
LIN W Q, WANG H, LIU J H. Research on active defense technology in network security based on non-cooperative dynamic game theory [J]. Journal of Computer Research and Development, 2013, 48(2): 306-316.

[10] BURKE D. Towards a game theory model of information warfare [D]. Montgomery: Air University, 2013.

[11] 刘玉岭, 冯登国, 吴丽辉. 基于静态贝叶斯博弈的蠕虫攻防策略绩效评估[J].软件学报, 2013, 23(3): 712-723.
LIU Y L, FENG D G, WU L H. Performance evaluation of worm attack and defense strategies based on static Bayesian game [J]. Journal of Software, 2013, 23(3): 712-723.

[12] GAO X, ZHU Y F. DDoS defense menchanism analysis based on signaling game model[C]//The 5th International Conference on the Computer Security Institute. San Francisco, c2013: 414-417.

[13] LIN J Q, LIU P, JING J W. Using signaling games to model the multi-step attack-defense scenarios on confidentiality[J]. Security Lecture Notes in Computer Science, 2014, 39(6): 118-137.

[14] 石乐义, 姜蓝蓝, 贾春福. 蜜罐诱骗防御机理的博弈理论分析[J]. 电子与信息学报, 2012, 34(6) :1420-1424.
SHI L Y, JING L L, JIA C F. A game theoretic analysis for the honeypot deceptive mechanism[J]. Journal of Electronics & Information Technology, 2012, 34(6) :1420-1424.

[15] 王元卓, 于建业, 邱雯. 网络群体行为的演化博弈模型与分析方法[J]. 计算机学报, 2015, 38(2) :282-300.
WANG Y Z YU J Y, QIU W. Evolutionary game model and analysis methods for network group behavior[J]. Chinese Journal of Computers,

2015, 38(2): 282-300.

[16] BABAR S D, PRASAD N R, PRASAD R. Game theoretic modeling of WSN jamming attack and detection mechanism[J]. Wire Multimedia Communications, 2013, 6983(6): 1-5.

[17] ROY S, ELLIS C, SHIVA S, et al. A survey of game theory as applied to network security[C]//The 47rd Hawaii International Conference on System Sciences. Washington D C, c2014: 15-24.

[18] FUDENBERG D, TIROLE J. Game theory[M]. Boston: Massachusettes Institute of Technology Press, 2012.

[19] **高志伟, 姚尧, 饶飞, 等. 基于漏洞严重程度分类的漏洞预测模型**[J].**电子学报**, 2014,41(9) :1785-1787.
GAO Z W, YAO Y, RAO F, et al. Predicting model of vulnerabilities based on the type of vulnerability severity[J]. Acta Electronica Sinica, 2014,41(9) :1785-1787.

[20] KAYODE, A B, BABATUNDE I G, HARUNA D I. DGM approach to network attacker and defender strategies[C]//The 19th International Conference for Digital Object. New York, c2014: 313-320.

[21] GORDON L, LOEB M, LUCYSHYN W, et al. 2014 CSI/FBI computer crime and security survey[C]//The Computer Security Institute. San Francisco, c2014: 11-34.

[22] SI P, ZHANG Q, YV F R. QoS aware dynamic resource management in heterogeneous mobile cloud computing networks[J]. China Communications, 2014: 41(5): 144-159.

[23] CVSS:national Nulnerability database version 2.5 [EB/OL]. http://nvd.nis.gov.

作者简介：

张恒巍（1978-），男，河南洛阳人，博士，信息工程大学讲师，主要研究方向为网络安全行为分析、信息安全风险评估。

余定坤（1991-），男，江西赣州人，信息工程大学硕士生，主要研究方向为信息安全风险评估。

韩继红（1966-），女，山西定襄人，博士，信息工程大学教授、博士生导师，主要研究方向为网络与信息安全、网络协议分析。

王晋东（1966-），男，山西洪桐人，信息工程大学教授，主要研究方向为网络与信息安全、云资源管理。

李涛（1992-），男，甘肃甘谷人，信息工程大学硕士生，主要研究方向为网络安全主动防御。