基于MAS的复杂网络安全形式化建模

危美林[1] 张明清[1] 唐 俊[2] 孔红山[1]
(信息工程大学 郑州 450001)[1] (清华大学 北京 100084)[2]

摘 要 针对网络攻击和防御形式化建模逼真度低和描述不规范的问题,基于多Agent建模思想提出了一种"微-宏"观相结合的具有良好扩展性的形式化建模方法,该方法从微观上描述了个体Agent的静态属性和动态行为,从宏观上描述了角色分配方式和各Agent之间的联系。接着以DDoS攻击与防御为例,给出了上述方法的具体实现过程。最后,仿真验证了DDoS攻防模型的正确性和有效性。

关键词 复杂网络安全,建模与仿真,智能体形式化建模,分布式拒绝服务攻击
中图法分类号 TP391.9 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.3.021

Formal Modeling of Complex Network Security Based on MAS

WEI Mei-lin[1] ZHANG Ming-qing[1] TANG Jun[2] KONG Hong-shan[1]
(The PLA Information Engineering University, Zhengzhou 450001, China)[1] (Tsinghua University, Beijing 100084, China)[2]

Abstract For the low fidelity and non-normative description of formal modeling of network attack and defense, a micro-macro combining formal modeling method with good scalability was proposed based on multi-Agent, which describes the static properties and dynamic behavior of individual agent from the microcosmic and describes the methods of role allocation and contacts between each agent from the macroscopic. Then, taking the DDoS attack and defense as example, we gave specific implementation process of the above method. Finally, a simulation of DDoS attack and defense was implemented to verify the model.

Keywords Complex network security, Modeling and simulation, Agent formal modeling, Distribution denial of service attack(DDoS)

1 引言

复杂网络是一种具有开放性、动态性、智能性、适应性和非线性等特点的网络,属于典型的复杂适应系统(Complex Adaptive System,CAS)。基于Agent的建模方法为CAS的研究提供了有力的手段[1]。复杂网络一旦遭受恶意攻击,将严重降低资源的可用性和用户的信任度与满意度[2],而在现实环境中进行复杂网络的攻防研究存在一定风险,建模与仿真为复杂网络的攻防研究提供了思路和方法。

目前,在多Agent系统(Multi-Agent System,MAS)的设计和开发中,主要有非形式化和形式化两大类建模方法。前者简单易用、直观明了,但是无法准确地描述MAS及其关键特性,对其理解也主要依赖于开发者的经验和知识。后者可以对MAS进行精确、无歧义的描述,且提供系统模型模拟和验证的分析手段和工具,有助于架起理论研究与工程实践之间的桥梁。蔡远利[3]指出5类典型的形式化建模方法不仅在Agent的形式化模型和仿真实现之间存在较大的差距,而且大多数方法仅局限于刻画Agent的静态属性。网络安全建模与仿真专家Igor Kotenko[4-6]基于MAS和OMNeT++网络仿真平台,对网络攻防建模与仿真做了大量研究,但其只是将攻击设备和防御设备抽象为Agent,缺乏对个体Agent的微观行为属性等的描述,建模粒度较粗。揣迎才[7]深入研究了Agent的自主行为和交互行为形式化建模方法,但是缺乏对防御团队之间的行为关系的宏观描述。

本文在前人研究的基础上,提出了一种"微-宏"观相结合的形式化建模方法,同时以DDoS攻防为例,给出了该方法的具体实现过程。最后,基于OMNeT++仿真平台,对DDoS攻防模型的正确性和有效性进行了验证。

2 MAS的形式化建模方法

针对网络攻击和防御形式化建模逼真度低和描述不规范的问题,本文提出一种"微-宏"观(即个体-团队)相结合的形式化建模方法,该方法不仅刻画了个体Agent的静态属性和动态行为,同时描述了不同类型的Agent之间交互协作的关系,易于实现系统模型向仿真语言的转换。

2.1 Agent个体层形式化建模方法

个体Agent的形式化描述可以采用一个四元组的形式:

$$A=\langle role, res, AB, IB\rangle \quad (1)$$

到稿日期:2014-04-20 返修日期:2014-06-18

危美林(1989-),女,硕士生,主要研究方向为信息栅格网络安全建模与仿真,E-mail:zhangmingqingwml@126.com;张明清(1961-),男,副教授,主要研究方向为系统建模与仿真;唐 俊(1976-),男,博士生,副教授,主要研究方向为系统工程;孔红山(1981-),男,硕士,讲师,主要研究方向为系统建模与仿真。

其中：(1)*role* 为 Agent 的角色名，它不仅提供了一个标识，也反映了该角色的工作类型。如角色名为 detector 的 Agent一般从事检测性工作。

(2)*res* 表示 Agent 拥有的全部资源，即可以被 Agent 用来完成进攻或防御的消息集合。在不同的攻防阶段，所需利用的资源也发生着变化。

(3)$AB=\{AB_1,AB_2,\cdots,AB_m\}$表示 Agent 的自主行为，是 Agent 所有自主子行为的集合。

(4)$IB=\{IB_1,IB_2,\cdots,IB_n\}$表示 Agent 的交互行为，是 Agent 所有交互子行为的集合。

2.1.1 Agent 自主行为建模

对 Agent 自主行为的形式化描述可以采用以下形式：

$$AB=\langle E,S,Q,\psi\rangle \tag{2}$$

式中，E 为 Agent 所有事件的集合；S 为 Agent 执行自主行为过程中所有状态的集合；Q 为所有自主动作元素构成的可能的时间序列或动作序列的集合，是 Agent 采取具体动作时的一种约束条件，用于控制 Agent 内部的行为细节，如发起某个动作的时机；ψ 是一个状态转换函数(见式(3))，表示 Agent 在自身产生的事件和动作序列的共同刺激下，由一个状态转换成另一个状态。其中，$e\in E,q\in Q,s_i,s_{i+1}\in S$ 均为变量。

$$\psi:E\times Q\times S_i\rightarrow S_{i+1}\quad \psi(e,q,s_i)=s_{i+1} \tag{3}$$

2.1.2 Agent 交互行为建模

对 Agent 交互行为的形式化描述可以采用以下形式：

$$IB=\langle E'_{in},E'_{out},S',Q',\psi'\rangle \tag{4}$$

式中，E'_{in}表示 Agent 所有输入事件的集合；E'_{out}表示 Agent 所有输出事件的集合；S'表示 Agent 与其它 Agent 交互过程中所有状态的集合；Q'表示所有交互动作元素构成的可能的动作序列集合，它是 Agent 采取具体动作时的一种约束条件，用于控制 Agent 间的交互细节，如交互时机和交互动作的有序排列；ψ'是一个事件转换函数(见式(5))，表示 Agent 处于某一内部状态时，输入事件到达，触发一个动作序列，之后产生一个输出事件。其中，$e'_{in}\in E'_{in},q'\in Q',s'\in S',e'_{out}\in E'_{out}$均为变量。

$$\psi':E'_{in}\times Q'\times S'\rightarrow E'_{out}\qquad \psi'(e'_{in},q',s')=e'_{out} \tag{5}$$

2.2 Agent 团队层形式化建模方法

攻击或防御团队的形式化描述可以采用以下形式：

$$G=\langle\Sigma,\Pi,\Phi,R,R'\rangle \tag{6}$$

其中：(1)$\Sigma=\{role_1,role_2,\cdots,role_k\}$表示攻防团队中角色的集合，$k\in N$是一个自然数，标识攻防团队中角色的个数。

(2)$\Pi=\{a_1,a_2,\cdots,a_l\}$表示攻防团队中 Agent 的集合，$l\in N$是一个自然数，标识攻防团队中某个角色所包含的 Agent 个数。

(3)$\Phi:\Sigma\rightarrow\Pi$是一个角色分配函数，调用 Φ 函数，可将 $G.\Sigma$中的角色 $role_i$ 分配给团队 $G.\Pi$ 中能够胜任的 Agent a_j，一个角色可以分配给多个 Agent，但一个 Agent 只能对应一个角色。

(4)$R=(r_{ij})$表示该 Agent 与团队内部其他 Agent 的关系，是一个二维矩阵(见式(7))，$i,j=1,2,\cdots,n,n\in N$是一个自然数，标识团队内部 Agent 的个数。r_{ij}只有两种取值即 0 或 1，0 代表 $Agent_i$ 和 $Agent_j$ 之间无交互，1 代表存在交互关系。

$$(r_{ij})=\begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1n}\\ r_{21} & r_{22} & \cdots & r_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ r_{n1} & r_{n2} & \cdots & r_{nn}\end{bmatrix} \tag{7}$$

(5)$R'\subseteq\Sigma\times\Sigma$是一个团队之间的交互关系集，当所有角色和 Agent 都存在一对一关系时，有 $R'\subseteq\Pi\times\Pi$。

3 DDoS 攻防 Agent 建模

上述提出的基于 Agent 的攻防模型形式化描述方法具有一定的通用性和可扩展性，对于新的攻击和防御类型的加入，只需要在相应的 Agent 模型中增加新的子行为即可。下面以 DDoS 为例给出攻防双方在此模型下的初始化和运行过程。

3.1 DDoS 攻击 Agent 建模

大型运营商互联网数据中心 IDC 在 2013 年发布的研究报告“全球攻击防御产品和服务 2013－2017 年预测”中预测称，在 2012 年到 2017 年间最常见的 DDoS 攻击类型仍然是“流量型”攻击。因此本文采用“流量型”攻击方式。

3.1.1 攻击 Agent 个体层建模

按照本文提出的个体 Agent 形式化建模方法，对攻击 Agent建模进行说明，如表 1、表 2 所列。

表 1 攻击 Agent 模型

符号	实例说明
角色名 role	attack
资源 res	res_1：数据包
自主行为 AB	AB_1：作为普通主机，请求并接收网络服务； AB_2：作为攻击机，产生大量异常网络流量，攻击目标服务器 Target
交互行为 IB	无

注：在 DDoS 实施过程中，一般是由一台主控机控制多台独立的“肉鸡”，此处的攻击 Agent 代表“肉鸡”。

表 2 A_{attack}的自主行为AB_2模型

符号	实例说明
事件 E	E_1：攻击控制指令到达
状态 S	S_1：idle； S_2：以真实地址向 Target 发送高频率的数据包； S_3：随机选取网络中合法主机的 IP 地址作为源地址，向 Target 发送高频率的数据包； S_4：随机选取地址作为源地址，向 Target 发送高频率的数据包； S_5：选取网络中合法主机的 IP 地址作为固定源地址，向 Target 发送高频率的数据包
时间序列 Q	$Q_1:t_1;Q_2:t_2;Q_3:t_3;Q_4:t_4;Q_5:t_5$
状态转换函数 ψ	$\psi_1:E_1\times Q_1\times S_1\rightarrow S_2;\psi_2:E_1\times Q_2\times S_1\rightarrow S_3;$ $\psi_3:E_1\times Q_3\times S_1\rightarrow S_4;\psi_4:E_1\times Q_4\times S_1\rightarrow S_5$

注：idle 表示空闲状态，t_1,t_2,t_3,t_4,t_5 无时间先后之分，且可重复执行某项活动，由仿真实验中的攻防想定而定。

3.1.2 攻击 Agent 团队层建模

按照上述提出的 Agent 团队形式化建模方法，对攻击 Agent团队建模进行说明。

攻击团队 $G_{attack}=\langle\Sigma,\Pi,\Phi,R,R'\rangle$中各元素描述如下：

$\Sigma=\{attack\}$；

$\Pi=\{A_{attack_1},A_{attack_2},\cdots,A_{attack_k}\}$，$k\in N$是一个自然数；

$\Phi(\{attack\})=\{A_{attack_1},A_{attack_2},\cdots,A_{attack_k}\}$；

$R=R'=\phi$，表示攻击团队内部和团队之间均无交互协作关系。

3.2 DDoS防御Agent建模

协同防御[8]为解决复杂网络环境下的DDoS攻击提供了一种有效的手段。在此，DDoS协同防御分为团队内和团队间防御两个层面，防御团队主要由防火墙Agent(A_{filter})、入侵检测Agent($A_{detector}$)和入侵追踪Agent($A_{investigator}$)等[9]组成。

3.2.1 防御Agent个体层建模

按照提出的个体Agent形式化建模方法，以入侵检测Agent为例，对防御Agent建模进行说明，如表3－表5所列。

表3 入侵检测Agent模型

符号	实例说明
角色名 role	detector
资源 res	res_1：自学习控制指令； res_2：数据包； res_3：协同控制指令； res_4：入侵检测协同请求消息； res_5：入侵检测协同消息； res_6：入侵警报消息
自主行为 AB	AB_1：防御知识自学习； AB_2：入侵检测
交互行为 IB	IB_1：与 A_{filter} 协同； IB_2：与 $A_{investigator}$ 协同； IB_3：与其它入侵检测 Agent($A_{detector}$)协同

表4 $A_{detector}$的自主行为AB_2模型

符号	实例说明
事件 E	E_1：res_1 到达；E_2：res_2 到达
状态 S	S_1：idle；S_2：BPS；S_3：SIPM；S_4：HCF
动作序列 Q	Q_1：提取数据包特征； Q_2：按照入侵检测规则进行异常匹配
状态转换函数 ψ	ψ_1：$E_2\times\{Q_1,Q_2\}\times S_1\rightarrow S_2$； ψ_2：$E_2\times\{Q_1,Q_2\}\times S_2\rightarrow S_3$； ψ_3：$E_2\times\{Q_1,Q_2\}\times S_3\rightarrow S_4$

注：idle表示无防御状态，BPS(bit per second)、SIPM(source IP monitoring)和HCF(hop count filtering)是3种检测强度渐增的检测状态。

表5 $A_{detector}$的交互行为IB_3模型

符号	实例说明
输入事件 E'_{in}	E'_{in1}：res_3 到达；E'_{in2}：res_4 到达；E'_{in3}：res_5 到达；E'_{in4}：res_6 到达；E'_{in5}：自生成 res_3；E'_{in6}：自生成 res_4；E'_{in7}：自生成 res_5；E'_{in8}：自生成 res_6
输出事件 E'_{out}	E'_{out1}：res_3 输出；E'_{out2}：res_4 输出；E'_{out3}：res_5 输出；E'_{out4}：res_6 输出
状态 S′	S_1'：idle
动作序列 Q′	Q_1'：存储并更新入侵检测知识库； Q_2'：提取本地入侵检测知识库相关内容； Q_3'：发送消息
状态转换函数 ψ'	ψ_1'：$E'_{in5}\times Q_3'\times S_1'\rightarrow E'_{out1}$； ψ_2'：$E'_{in6}\times Q_3'\times S_1'\rightarrow E'_{out2}$； ψ_3'：$E'_{in7}\times Q_3'\times S_1'\rightarrow E'_{out3}$； ψ_4'：$E'_{in1}\times\{Q_2',Q_3'\}\times S_1'\rightarrow E'_{out3}$； ψ_5'：$E'_{in2}\times\{Q_2',Q_3'\}\times S_1'\rightarrow E'_{out3}$； ψ_6'：$E'_{in3}\times\{Q_1',Q_2',Q_3'\}\times S_1'\rightarrow E'_{out3}$； ψ_7'：$E'_{in4}\times\{Q_2',Q_3'\}\times S_1'\rightarrow E'_{out3}$； ψ_8'：$E'_{in8}\times Q_3'\times S_1'\rightarrow E'_{out4}$

3.2.2 防御Agent团队层建模

按照上述提出的Agent团队形式化建模方法，对防御Agent团队建模进行说明。

防御团队$G_{defender}=\langle\Sigma,\Pi,\Phi,R,R'\rangle$中各元素描述如下：

$\Sigma=\{filter,detector,investigator\}$，防御团队包括过滤防火墙、入侵检测和入侵追踪3种角色；

$$\Pi=\{A_{filter_1},A_{filter_2},\cdots,A_{filter_l},A_{detector_1},A_{detector_2},\cdots,A_{detector_m},A_{investigator_1},A_{investigator_2},\cdots,A_{investigator_n}\}$$

$l,m,n\in N$均为自然数；

$\Phi(\{filter\})=\{A_{filter_1},A_{filter_2},\cdots,A_{filter_l}\}$

$\Phi(\{detector\})=\{A_{detector_1},A_{detector_2},\cdots,A_{detector_m}\}$

$\Phi(\{investigator\})=\{A_{investigator_1},A_{investigator_2},\cdots,A_{investigator_n}\}$；

$R=\begin{bmatrix}1&0&0\\1&1&1\\1&1&1\end{bmatrix}$，$A_{detector}$发现攻击时，向防御团队内部的$A_{filter}$和$A_{investigator}$发送警报消息，$A_{investigator}$追踪到攻击源时，发送追踪成功消息通知$A_{filter}$和$A_{detector}$；

$$R'\subseteq\{(\{A_{filter_{l'}},A_{detector_{m'}},A_{investigator_{n'}}\},\{A_{filter_{l''}},A_{detector_{m''}},A_{investigator_{n''}}\})\}$$

其中，$l',l'',m',m'',n',n''\in N$，且$0\leqslant l',l''\leqslant l$，$0\leqslant m',m''\leqslant l$，$0\leqslant n',n''\leqslant l$，对于$A_{detector}$而言，$A_{detector}\neq\varnothing$，表明$A_{detector_{m'}}$与$A_{detector_{m''}}$之间存在交互协作关系。

4 仿真实验与结果分析

4.1 仿真实验设计

为验证DDoS攻防模型的有效性，基于OMNeT++[10]设计的仿真系统主要包括攻击模拟仿真子系统、协同防御仿真子系统和业务仿真子系统。其中，设定attack总数$k=4$，filter总数$l=7$，detector总数$m=7$，investigator总数$n=7$，Server1－Server3为服务器，target为受害端，Cli_1－Cli_21为客户端主机，R1－R11为路由器，构建的DDoS攻防场景如图1所示，图中黑圈内的仿真设备组成一个防御团队。

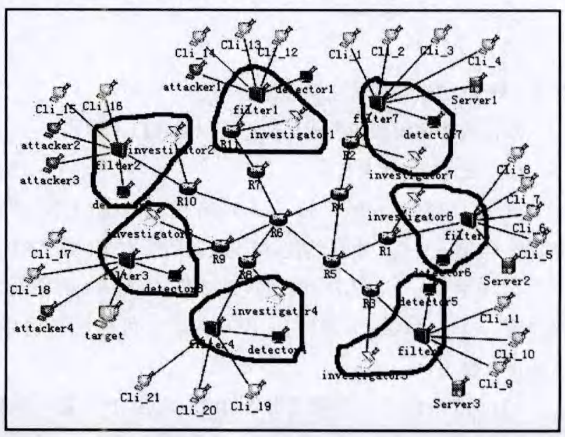

图1 DDoS攻防仿真拓扑

复杂网络下的攻防想定：设置仿真时间为300s。attack1－attack4在$t_1\in[0,80)$s内向target发送正常的业务消息；在t_2

$\in[80,140)$s 内向 target 发送无地址欺骗的攻击消息；在 $t_3\in[140,200)$s 内向 target 发送随机地址欺骗的攻击消息；在 $t_4\in[200,260)$s 内向 target 发送半随机地址欺骗的攻击消息；在 $t_5\in[260,300]$s 内向 target 发送固定地址欺骗的攻击消息。detector1－detector7 在 $t_6\in[0,50)$s 内进行 BPS、SIPM 和 HCF 防御知识自学习；在 $t_7\in[50,300]$s 内处于 DDoS 攻击检测阶段；filter1－filter7 提取数据包特征与安全策略库进行匹配，实现过滤功能；investigator1－investigator7 的主要目的是事后追踪取证；Server1－ Server3 主要提供 HTTP 业务服务。

4.2 仿真运行与结果分析

收集 detector3 在防御知识自学习模式下的相关数据，如图 2 所示。该日志主要记录了合法主机地址、相应跳数以及标准数据传输速率等信息，在攻击防御模式下被调用。

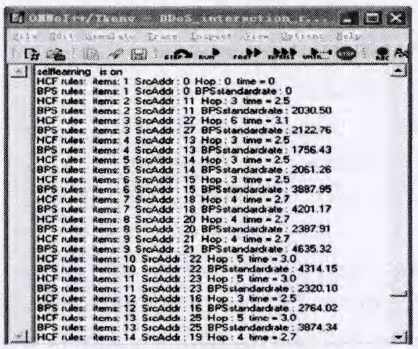

图 2 detector3 自学习阶段(部分)

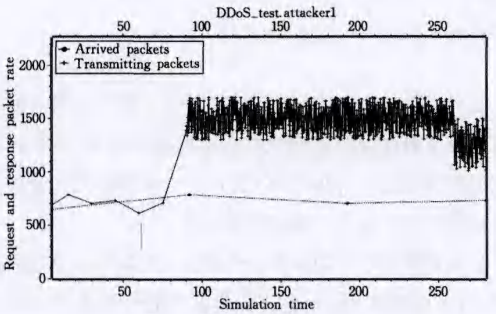

图 3 attack1 请求/回应数据包速率

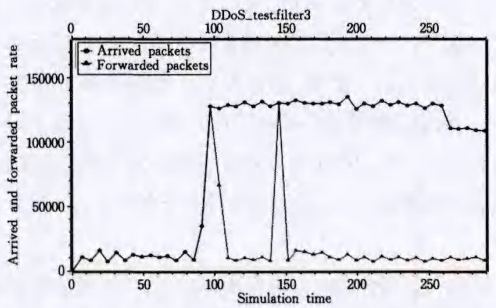

图 4 filter3 输入/输出数据包速率

下面以 attack1 和 filter3 为例，分析仿真结果，并对复杂网络下的攻防行为作进一步验证和分析。如图 3 所示，从 80s 之后，attack1 发送的数据包量远远大于接收的数据包量，验证了攻击方实施了“流量型”DDoS 攻击，且由图 3 可知前 3 种攻击方式效果相当，攻击流量均高于第四种攻击的攻击流量。如图 4 所示，当攻击开始后，filter3 在 96s 时才接收到 detector3 传来的入侵警报消息，145s 时接收到另一种入侵警报消息，并且由图 4 可知，后两种攻击方式均属于第二种攻击的特殊情况，进行 BPS、SIPM 和 HCF 算法过滤后，filter3 输出的数据包流量基本恢复正常。

结束语 本文基于 Agent 提出了一种“微-宏”观相结合的形式化建模方法，该方法考虑的因素全面，易于实现系统模型向仿真语言的转换。同时以 DDoS 攻击为例，给出了攻防双方采用上述形式化建模方法的具体实现过程。最后，OMNeT++仿真验证了 DDoS 攻防模型的正确性和有效性。下一步我们将继续研究和扩展复杂网络攻击和防御 Agent 形式化建模中尚未考虑的因素，例如减少防御 Agent 交互协作产生的负载量问题和防御 Agent 团队之间交互协作的信任问题等。

参 考 文 献

[1] Holland J H. Adaptation in natural and artificial systems: An introductory analysis with applications to biology, control, and artificial intelligence [M]. U Michigan Press, 1975

[2] Varalakshmi P, Selvi S T. Thwarting DDoS attacks in grid using information divergence [J]. Future Generation Computer Systems, 2013, 29(1): 429-441

[3] 蔡远利，于振华，张新曼. 多 Agent 系统形式化建模方法研究[J]. 系统仿真学报，2007，19(14)：3151-3157

[4] Kotenko I, Konovalov A, Shorov A. Agent-based simulation of cooperative defence against botnets[J]. Concurrency and Computation: Practice and Experience, 2012, 24(6): 573-588

[5] Kotenko I, Konovalov A, Shorov A. Agent-based Modeling and Simulation of Botnets and Botnet Defense[C]// Conference on Cyber Conflict. 2010: 21-24

[6] Kotenko I, Konovalov A, Shorov A. Simulation of Botnets: Agent-based approach[M]// Intelligent Distributed Computing IV. Springer Berlin Heidelberg, 2010: 247-252

[7] 揣迎才，张明清，唐俊，等. 基于 Agent 的 DDoS 协同防御实体行为建模[J]. 计算机工程，2013，39(6)：158-161

[8] Lee S B, Kang M S, Gligor V D. CoDef: collaborative defense against large-scale link-flooding attacks[C]// Proceedings of the ninth ACM conference on Emerging networking experiments and technologies. ACM, 2013: 417-428

[9] 张明清，揣迎才，唐俊，等. 一种 DRDoS 协同防御模型研究[J]. 计算机科学，2013，40(9)：99-102

[10] 夏锋. OMNeT++网络仿真[M]. 北京：清华大学出版社，2013