Journal of System Simulation

Volume 30 | Issue 9 Article 4

1-8-2019

Modeling and Simulation on Entities' Belief in Cyberspace

Jiuyang Tao
1. Department of Information Operation & Command Training, National Defense University, Beijing 100091, China;;2. College of Command Information Systems, PLA University of Sci. & Tech., Nanjing 210007, China;

Wu Lin
1. Department of Information Operation & Command Training, National Defense University, Beijing 100091, China;;

Xiaoyuan He
1. Department of Information Operation & Command Training, National Defense University, Beijing 100091, China;;

Rong Ming
1. Department of Information Operation & Command Training, National Defense University, Beijing 100091, China;;

Modeling and Simulation on Entities' Belief in Cyberspace

Abstract

Abstract: Of all cyber-attacks, 'fabrication' which is aimed at impacting one's awareness is becoming the common means, so it is of great importance to explore ways so as to defend such attacks. An attack can success or not always rely on the entities' belief of certain events. In this paper, two different ways of 'fabrication' attack are put forward, and three essential conditions for 'fabrication' attack are analyzed. *Second, a cyberspace belief model in terms of the Dempster-Shafer framework based on situation awareness theory is built to study the evolution of the cyber entities' belief under the* 'fabrication' *attack.* In addition, an algorithm used to compound D-S belief values among entities in cyberspace is designed. At last, the combination and evolution of D-S belief are studied on the scale-free network and the small world network, three conclusions are proposed at last.

Keywords

cyberspace, Dempster-Shafer evidence theory, complex networks, situation awareness

Recommended Citation

Tao Jiuyang, Wu Lin, He Xiaoyuan, Rong Ming. Modeling and Simulation on Entities' Belief in Cyberspace[J]. Journal of System Simulation, 2018, 30(9): 3255-3263.

第 30 卷第 9 期 系统仿真学报© Vol. 30 No. 9
2018 年 9 月 Journal of System Simulation Sep., 2018

网络空间实体信度演化模型及其仿真

陶九阳[1,2]，吴琳[1]，贺筱媛[1]，荣明[1]
(1. 国防大学信息作战与指挥训练教研部，北京 100091；2. 解放军理工大学指挥信息系统学院，江苏 南京 210007)

摘要：“伪造”已经成为一种常见的网络攻击方式。研究针对“伪造”攻击的防御措施具有重要意义。“伪造”攻击依赖网络对伪造信息的信(任)度。提出了两种“伪造”攻击方式，并分析了“伪造”攻击的三个必要条件；*根据 D-S 证据理论，建立了网络空间实体对事件的信度模型，设计了面向态势感知共享的网络空间信度合成算法，研究了“伪造”导致的网络实体信度的演化；*仿真分析了“伪造”在无尺度网络和小世界网络上的信度合成和演化，得到了网络空间中信度演化的三个结论。

关键词：网络空间；D-S 证据理论；复杂网络；态势感知
中图分类号：TP391.9 文献标识码：A 文章编号：1004-731X (2018) 09-3255-09
DOI: 10.16182/j.issn1004731x.joss.201809004

Modeling and Simulation on Entities' Belief in Cyberspace

Tao Jiuyang[1,2], *Wu Lin*[1], *He Xiaoyuan*[1], *Rong Ming*[1]
(1. Department of Information Operation & Command Training, National Defense University, Beijing 100091, China;
2. College of Command Information Systems, PLA University of Sci. & Tech., Nanjing 210007, China)

Abstract: Of all cyber-attacks, 'fabrication' which is aimed at impacting one's awareness is becoming the common means, so it is of great importance to explore ways so as to defend such attacks. An attack can success or not always rely on the entities' belief of certain events. In this paper, two different ways of 'fabrication' attack are put forward, and three essential conditions for 'fabrication' attack are analyzed. *Second, a cyberspace belief model in terms of the Dempster-Shafer framework based on situation awareness theory is built to study the evolution of the cyber entities' belief under the* 'fabrication' *attack.* In addition, an algorithm used to compound D-S belief values among entities in cyberspace is designed. At last, the combination and evolution of D-S belief are studied on the scale-free network and the small world network, three conclusions are proposed at last.

Keywords: cyberspace; Dempster-Shafer evidence theory; complex networks; situation awareness

引言

对网络空间攻击破坏行为进行建模仿真研究，是提升网络空间安全的重要手段之一。网络攻击通常可以分为网络信息资源的退化、中断、篡改、伪造、冒用和窃取六大类[1-2]。目前，国内外网络攻击建模领域的研究，针对信息资源的退化、中断、窃密等面向物理域和信息域的网络攻击建模仿真有一些报道，但面向实体态势感知和认知的伪造欺骗类网络攻击建模仿真却鲜有披露。

所谓伪造，就是攻击者将捏造的信息注入被攻击者系统，对被攻击者进行欺骗、诱导以达成攻击目的。这种攻击行为往往造成被攻击者的感知和认知错误，从而做出攻击者希望的决策和行为。2014

收稿日期：2016-03-10 修回日期：2016-09-10;
基金项目：军民共用重大研究计划联合基金(U1435218), 国家自然科学基金(61174156, 61273189, 61174035, 61374179, 61403400, 61403401);
作者简介：陶九阳(1983-)，男，山东五莲，博士生，研究方向为运筹分析与军事智能决策。

年，俄罗斯乌克兰克里米亚争端中，克里米亚前线的乌克兰指挥官收到了互相矛盾的命令，产生了认知混乱，从而扰乱了指挥控制活动的有效实施。因特网中一些误导民众的谣言，广义上讲也属于这一类攻击行为。近来，认知人工智能快速发展，如围棋人工智能AlphaGo[3]，微软智能图像识别，以及IBM智能问答系统“沃森’等，可以预见，未来具有认知能力的无人系统会大量出现并协同工作，伪造攻击会成为具有认知能力的智能化系统面临的巨大安全隐患，因此预先研究面向认知的伪造攻击可能的攻击方式，探索防范伪造攻击的方法，具有重要意义。伪造攻击能否达成，与网络实体对伪造事件的信任程度有很大关系。本文考虑运用D-S证据理论中的信度(belief)[4]及其合成理论[4]，以网络实体态势感知、认知的共享为出发点，建模仿真网络空间实体对伪造事件的信度演化，以此来启发针对此类攻击的防御方法和措施。

1 网络空间伪造攻击模型分析

1.1 网络空间伪造攻击过程分析

网络空间伪造的一般过程是：攻击方首先根据自身的目的和被攻击方的特点，设计一个或多个伪造事件(或者信息)，选择一个或者多个入口，使伪造的事件进入被攻击者的网络空间。一旦攻击成功，被攻击者在察觉到事件后，会对事件进行理解和认知预测，并根据伪造的事件做出有利于攻击方的决策和行动。

经过分析可发现，这一过程中包含着一个Endsley 态势感知参考模型[6-7]与 Boyd 的OODA(Oberve、Orient、Decide、Act)环模型的混合过程。为了进一步分析这个过程，我们建立了如图 1 所示的网络空间实体间信息交互的 OODA 模型。模型主要包含三部分：第一是网络实体对事件进行感知，包括对事件的察觉，以及根据共有的知识库和私有知识库对事件的理解和预测；第二是根据感知结果进行决策，第三是根据决策作出行动，同时对网络空间形成影响。伪造能够破坏和影响对方的态势感知，而这种破坏性效果的达成，依赖于被攻击方在态势感知过程中对伪造事件的信任。

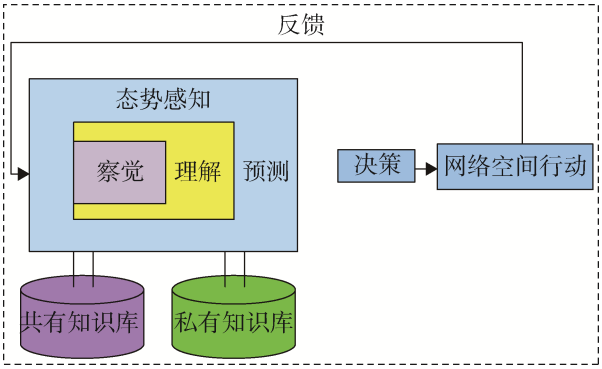


图1 网络空间实体OODA模型
Fig. 1 Cyberspace entity OODA model

对单个实体进行伪造攻击过程比较简单，只要使其对伪造事件足够信任。而现实中，更为普遍的是网络空间实体通过协同行动来共同完成任务。在这种情况下，伪造事件通常使众多网络实体对事件达成一致的信任来达到攻击目的。

众多网络实体要想实现协同行动，首先就需要进行广泛的共享态势感知和共享理解，然后进行决策做出行动。一致的态势感知就成为网络实体进行决策和协同行动的基础[8]。带有协同的网络实体态势感知过程包含两个方面：一方面，网络实体首先通过共有知识库进行判断和理解，然后通过自身的私有知识库对事件进行判断、理解及预测，并把感知结果共享给相邻的网络节点；另一方面，接收来自网络空间中其他节点的感知结果，与自身的感知结果进行融合，修正和完善自身的感知结果。

1.2 网络空间伪造攻击方式及模型

为了能够进一步模型化地分析网络空间伪造攻击方式，我们可以做出如下的假设。

假设1 共有知识库为所有网络实体共同使用，普通网络实体无权修改共有知识库的内容，只有特殊机构有权修改和更新其内容。私有知识库是网络实体通过自身积累获得，可以随时更新和修改其内容。

https://dc-china-simulation.researchcommons.org/journal/vol30/iss9/4
DOI: 10.16182/j.issn1004731x.joss.201809004

攻击方(Attacker)和被攻击方(Victim)分别用A、V来表示。假设V方网络空间中有 n 个网络实体，网络空间共有知识库为 R_G，第 i 个网络实体的私有知识库为 $R_i, i \in 1 \cdots n$。

A方通常通过情报、技术分析等手段获悉V方网络实体的知识库内容，根据知识库内容设计攻击策略，一般有两种攻击方式：

攻击方式1：根据众多网络实体的知识库设计伪造对A方有利的事件，使得V方网络实体对事件产生错误感知，从而采取错误的或者是A方期望的行动。这是一种在认知域上的行动，它通过对V方态势感知环节进行破坏，诱导V方进行错误决策的攻击或防御方式。

攻击方式2：A方通过分析V方网络实体的共有知识库 R_G 和私有知识库 $\{R_1, R_2, \cdots R_n\}$，伪造攻击事件，使得V方的感知结果出现严重的冲突，从而无法迅速达成一致的态势感知，迟滞V方决策制定速度和行动速度，为A方争取时间资源，前面介绍的俄罗斯对克里米亚的军事行动就属于此种类型。这是一种在认知域上的行动，A方通过对V方态势感知环节进行干扰破坏，来削弱V方决策能力的攻击方式。

假设每个知识库都有识别功能，知识库可以对事件的真假进行推理识别。如果认为一个事件为真，就说事件符合该知识库。对于攻击方式1，假设通过分析V方知识库，A方伪造出的事件为e。那么事件e须满足条件1和条件2。

条件1：e符合V方共有知识库。也就是伪造事件e不会和V方共有知识库产生冲突。此条件表示为式(1)：

$$\text{match}(R_G, e) \geqslant 1-\varepsilon \tag{1}$$

式(1)中match是一个匹配函数，表示事件在知识库上的符合程度，其值介于0和1之间，1表示完全符合，0表示完全不符合，值越大表示知识库对事件越信任。ε表示一个非常小的正数。式(1)表示几乎完全符合的条件。

条件2：e符合的私有知识库数目要超过某个数值。由于网络实体协同行动时，要进行态势感知的共享，如果e和太多私有知识库发生冲突，在网络实体共享事件过程中，事件e可能无法生存和产生影响效果。此条件表示为式(2)。

$$\begin{cases} \text{match}(R_i, e) \geqslant 1-\varepsilon_i \\ \quad \vdots \\ \text{match}(R_j, e) \geqslant 1-\varepsilon_j \\ \left| R_i \cdots R_j \right| \geqslant k \end{cases} \tag{2}$$

式中：k 为一个正整数，表示 k 个(含)以上网络实体认为事件 e 为真。k 的取值在实际应用中要根据实验或者经验给出，不同应用背景 k 取值可能相差很大。图 2 给出了攻击方式 1 的攻击过程示意图。

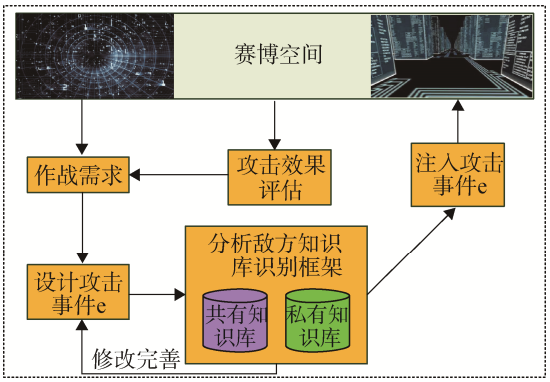


图2 攻击方式1的攻击过程示意图

Fig. 2 Schematic diagram of the attack process with mode 1

对于攻击方式2，A方通常根据V方知识库伪造出两个(或多个)虚假事件为e_1、e_2。e_1、e_2两个事件本身可能具有不一致性，即在一定程度上互相矛盾。与攻击方式1的原因相同，事件e_1、e_2首先都要满足条件1。另外，对于条件2，假设V方信任事件e_1而不信任e_2的网络实体数目为k_1， 信任e_2而不信任e_1的网络实体数目k_2。e_1、e_2进入V方的网络空间就会制造出不一致的态势感知结果，使V方产生认知混乱。因此要达成攻击方式2，还需要满足如下条件。

条件3：要使得相信e_1和相信e_2的网络空间实体数目要符合一定的规律。假设在联合行动中，态势感知的结果是少数服从多数，那么如果一方占据绝对优势，另一方就会服从占据绝对优势的一方，由

于在一些网络中，节点的影响力差异巨大，因此，这里的少数服从多数指的是综合影响力小的一方，服从影响力大的一方，而不单纯是计算节点的数目来衡量。从而形成较为一致的态势感知。此条件表示为式(3)。

$$\left|\sum_{i=1}^{k_1}\lambda_i-\sum_{j=1}^{k_2}\mu_j\right|\leqslant\varepsilon,\sum_{i=1}^{k_1}\lambda_i+\sum_{j=1}^{k_2}\mu_j=1 \tag{3}$$

公式(3)中，λ_i表示认同事件e_1的网络实体中第i个实体的影响力系数。μ_j表示认同事件e_2的网络实体中第j个实体的影响力系数。这里的影响力系数可能与节点的级别、度数等因素有关，级别越高度数越大的节点，其影响力系数通常也越大。ε表示一个非常小的数，ε 非常小表示二者影响力势均力敌。事实上，攻击方式2是攻击方式1的进一步拓展。本文以D-S证据理论的信度为基础来探讨攻击方式1会对网络空间产生的影响。

2 基于 D-S 证据理论网络空间实体信度模型

上述 A 方攻击方式 1 能够达成的一个关键，是使得 V 方能够相信伪造的事件。事实上，网络空间中实体对于一个事件的接受程度与对该事件的信任度密切相关。由于网络实体私有知识库不同，不同的网络实体对同一事件的信任度可能不同。因此，可以引入 D-S 证据理论的信度概念来对其进行形式化建模分析。

D-S 证据理论是 Dempster 和 Shafer 于 1976 年建立的数学理论，用于处理不确定性、不精确以及间或不准确的信息[9]。D-S 证据理论随后被广泛应用模糊推理、不确定性信息处理和人工智能等领域[10-11]。证据理论中引入了信度函数(belief function)来度量不确定性，从而为不确定事件的可信度分析提供了一个理论性的基础。借用 D-S 证据理论的信度概念，本文定义信度为网络实体对于某一不确定性事件的相信程度。

对于一个事件 e，设网络实体所能认识到的可能结果用集合Θ表示，集合Θ称为对事件 e 的识别框架。如果根据网络实体的知识库和其自身经验，可以得到一批针对该框架的证据，那么，根据 D-S 证据理论，就可以在框架Θ的所有幂集$\rho(\Theta)$上产生一个信度函数 mass(用 m 表示)，如公式(4)所示：

$$m:\rho(\Theta)\to[0,1],\text{且}m(\varphi)=0,\sum_{E\subseteq\Theta}\mathrm{m}(\mathrm{E})=1 \tag{4}$$

公式(4)用来表示实体对各个事件(或事件组合)的信任度的分配，例如天气预报预报有三个事件：下雨，阴天，晴天。则m(下雨)=0.3，就表示对下雨这个事件信任程度为0.3。信度函数m是一个介于0和1之间的数值，0表示完全不相信，1表示完全相信。数值越大相信程度越高。值得注意的是，m可以作用于事件的组合，即识别框架的幂集，如公式(4)中，如果E={下雨，阴天}，则m(E)=0.8表示对事件要么下雨要么阴天的信任度为0.8。

假设针对事件 e 的识别框架为 $\Theta=\{e,\bar{e}\}$，设 m_i 为网络实体 i 在识别框架Θ上的私有基本可信度分配，m_G 为 V 方网络空间在识别框架Θ上共有基本可信度分配。私有基本可信度和共有基本可信度的分配依据，来源于第 2 节中介绍的私有知识库和共有知识库假设。

假设，网络实体可以综合自身知识库的证据和邻居节点的感知结果进行融合识别。对于网络实体i，假设其邻居节点组成的集合为$\{a,\cdots,b\}$，则实体i对于事件e与其邻居进行相互印证融合后的信度$m_i(e)$可以根据Dempster-Shafer合成公式[6]得到，如公式(5)所示：

$$m_i(e)=(m_a\oplus\cdots\oplus m_b)(e)=\frac{1}{N}\sum_{\bigcap_{j=a}^{b}E_j=e}\prod_{j=a}^{b}m_j(E_j) \tag{5}$$

$$\text{其中 } N=\sum_{\bigcap_{j=a}^{b}E_j\neq\varphi}\prod_{j=a}^{b}m_j(E_j)>0 \tag{6}$$

假设2：为了保证感知结果的一致性和行动的一致性，假设网络空间中存在一个协调机构，对所有网络实体的感知结果进行分析和汇总后给出一致的感知结果，并且所有网络实体都接受网络协调

机构的最终感知结果。

例如在联合作战行动中，美军通用作战态势图(Common Operational Picture，简称COP)就扮演着网络协调机构类似的角色，所有作战实体都是通过COP进行一致的态势感知。

进一步假设，对于事件e，网络协调机构通过收集网络空间中实体的信度，来合成总的信度，其**信度合成算法**为：

Step1：根据公式(7)计算所有网络实体的平均信度值，公式(7)为：

$$m_S(e)=\frac{1}{n}\sum_{i=1}^{n}m_i(e) \tag{7}$$

Step2：将式(7)与共有知识库的基本信度 $m_G(e)$ 进行加权，根据公式(8)得到最终信度 $m_z(e)$为：

$$m_Z(e)=\alpha m_S(e)+\beta m_G(e)=$$
$$\alpha\frac{1}{n}\sum_{i=1}^{n}m_i(e)+\beta m_G(e),\alpha+\beta=1 \tag{8}$$

对于式(8)，α和β取值的大小，取决于网络协调机构对公有知识库的识别结果和私有知识库的识别结果的偏好。假定，当网络协调机构的最终信度不低于M时，即有：

$$\frac{1}{n}\sum_{i=1}^{n}m_i(e)+\beta m_G(e)\geq M \tag{9}$$

满足式(9)，网络协调机构就认为事件e为真，所有的网络实体就会相信事件e并根据事件e进行决策和行动。

因此，攻击方为了能够达成网络攻击目的，在伪造事件e时，相关的参数，需要满足公式(9)。然而，通常的情况下，A方伪造的事件e进入V方的网络，都会选定一个或几个入口节点来让事件在网络进行传播。那么，不同类型的网络，不同的入口节点选择下，即使初始信度分布相同，其信度合成演化结果也可能不同。

3 网络空间实体信度传播与合成算法

如前所述，网络空间中的众多实体在获知一个事件e的时候，对其信度可能不同。这时候，网络实体之间会相互求证，以此来更新对事件e的信度。例如，日常生活中我们得到一个关于某个事件的消息，但不确定是不是真的，此时我们通常会向朋友询问，如果大家都说是真的，无疑会增加我们对此事件的信任度，反之，会降低对此事件的信任度。这个过程就是信度的合成。通过信度合成，可以使得网络实体对于某一个事件得到进一步的确认或者否认。

假设伪造事件 e 随机地进入 V 方网络空间中的一个节点，因为网络对事件具有传播性，事件 e 会在 V 方网络进行传播。可以假设受攻击节点会将自身对于事件 e 的信度与周围的邻居节点合成。受攻击节点的邻居节点也重复此过程，最终，全网络的节点完成信度的合成。

具体信度传播和合成算法如下：

step1：为每个节点分配一个关于事件e的私有基本可信度 m_i，然后分配一个整个 V 方网络对事件 e 的共有基本可信度 m_G。m_i、m_G服从[0,1]均匀分布。将所有节点加入到“未访问队列”list 中。

step2：如果 list 不空，随机地在 list 中选择一个节点 v_i，按照第 3 节中提出的信度合成算法，将此节点与其邻居节点进行信度的合成。然后从 list 中将节点 v_i 移出。如果 list 为空，则转到 step5。

step3：从当前节点 v_i 的邻居节点中取出一个节点 v_j，检查 v_j 是否在队列 list 中，如果是，则继续执行 step4。如果不是，则重复执行 step3。如果所有 v_j 的邻居节点都已经访问完，则转到 step2。

step4：将新取出的节点 v_j 与其邻居节点按照公式(5)进行信度合成。合成完毕然后转到 step3。

step5：将所有的节点信度与共有知识库的基本信度 m_G 进行合成，仿真结束。

4 网络空间实体信度演化仿真分析

如果把每个网络实体看成一个抽象的节点，每两个实体之间的信息交互看成是一条连线，那么网络空间可以抽象出一个由节点和边组成的网络。而网络空间中网络的组织方式可能多种多样，组织结

构也异常复杂，不同的网络结构，对于同一个事件 e，其信度合成和演化也不同。因此，需要对具有不同结构的网络分别进行分析。由此我们引入复杂网络的理论方法来进行建模和仿真。

目前，随着对复杂网络的持续深入研究，发现很多网络都具有无尺度(Scale-Free)的特性[12]和小世界(Small World)特性[13]。本文以网络空间中具有 BA 无尺度特性的网络和 NW 小世界特性的网络为研究对象，对前面提出的网络伪造攻击模型进行仿真分析。

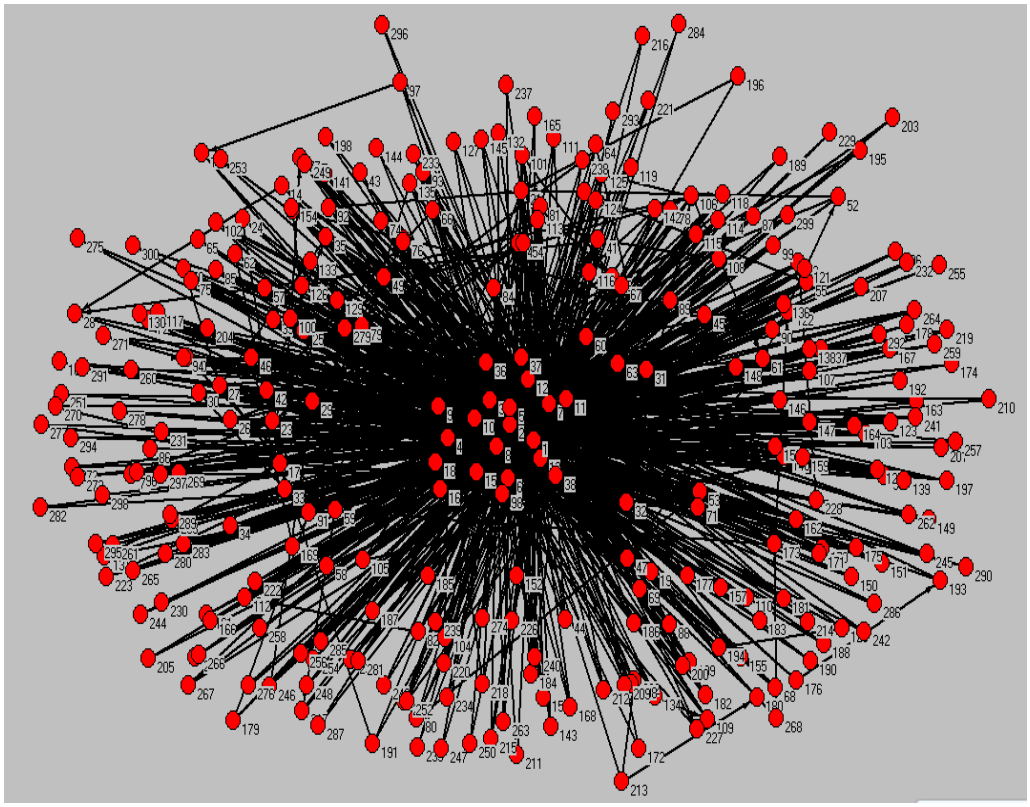
首先，按照 BA 无尺度模型的改进构造算法和 NW 小世界网络构造算法，分别构造一个拥有 300 个节点，平均度数为 6 的无尺度网络和小世界网络。如图 3 所示。

通过对比图 4 中(a)~(b)可以发现，BA 无尺度网络和 NW 小世界网络对于攻击事件 e，经过网络节点相互之间的信度合成后，节点的信度有收敛的现象，即信度合成后的方差变小。由此可以得到：

结论 1：基于前面假设产生的网络空间是合作型的，网络实体对事件 e 交换看法有消除分歧的作用。这里的合作型网络表示的是网络实体之间是普遍合作的，普遍乐于接受其他人的观点。现实生活中还存在一种非合作型网络，对于某些事件进行交流后，不仅不会使分歧减小，甚至会使分歧增大。我们通常说的“抬杠”就是这种情况。

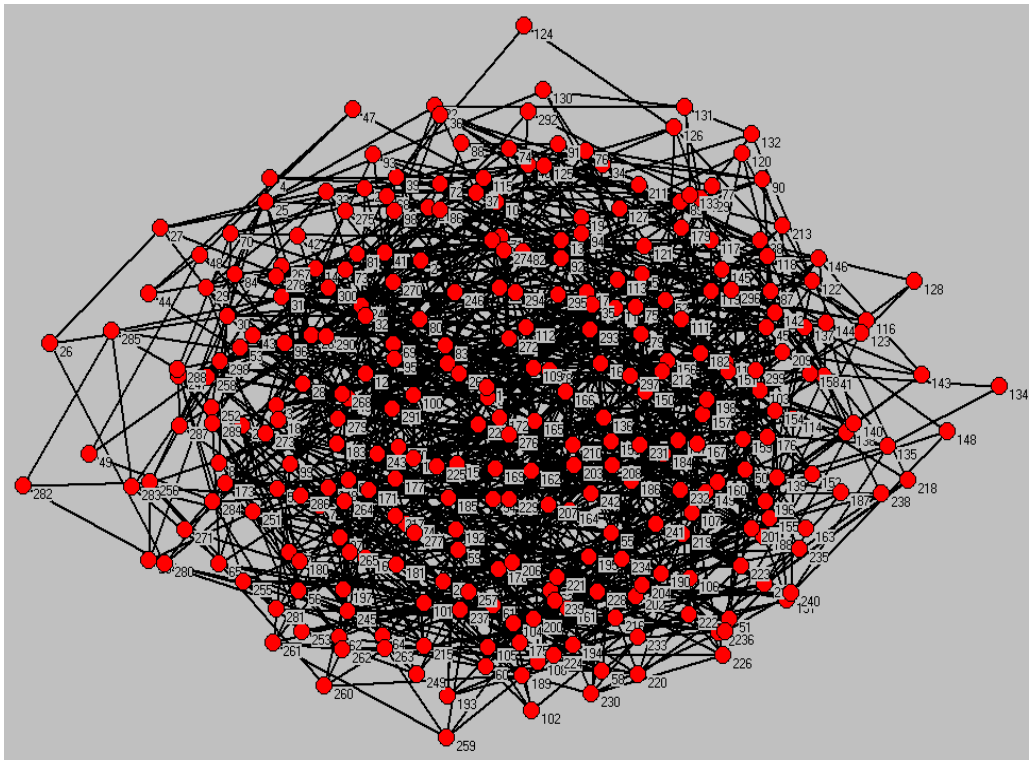
然后按照信度传播和合成算法，得到信度的演化结果如图 4 所示。

如果伪造的欺骗事件攻击入口节点不仅有一个，那么伪造事件可能在网络空间中进行多次传播。在现实中这种现象很多，例如在网络中你可能接收到多个好友关于某一事件的消息。针对这种现象，可以修改上述算法来近似呈现：step5 结束后不结束仿真，返回 step1，用 step5 中生成的信度，代替 step1 中的初始信度，进行仿真迭代。我们以图 3(b)所示的小世界网络为例，按修改的算法迭代三次，可以看到信度在小世界网络中的演化，得到图 5(a)所示结果。图 5(b)表示的是迭代 10 次，信度的标准差随着迭代次数增加的变化曲线。



(a) 无尺度网络模型

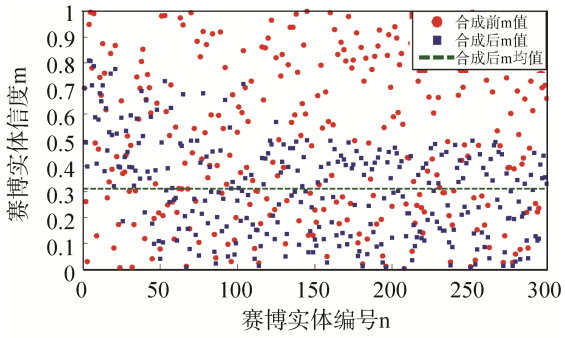
https://dc-china-simulation.researchcommons.org/journal/vol30/iss9/4
DOI: 10.16182/j.issn1004731x.joss.201809004



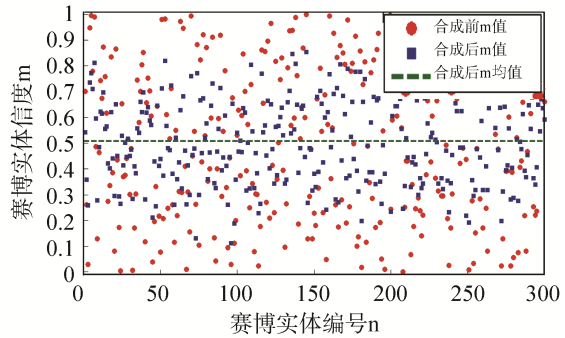
(b) 小世界网络模型

图 3 复杂网络模型

Fig. 3 Complex network model



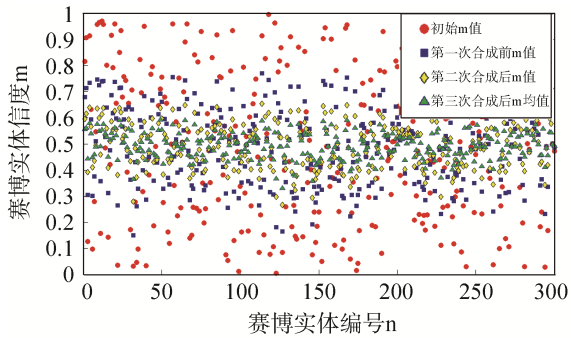
(a) 随机攻击无尺度网络信度合成前后分布对比图



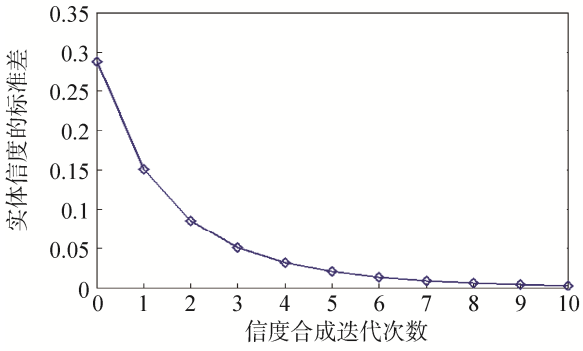
(b) 随机攻击小世界网络信度合成前后分布对比图

图 4 随机攻击复杂网络信度合成前后分布对比

Fig. 4 Comparison of distribution before and after random attack complex network reliability synthesis



(a) NW小世界网络信度演化



(b) 信度样本标准差变化曲线

图 5 信度演化及稳定性

Fig. 5 Reliability evolution and stability

对结果进行分析，可以得到：

结论 2：随着迭代次数的增加，各实体针对事件 e 的信度差异越来越小，而且这种减小的速度呈现指数下降趋势，这意味着各实体对于事件 e 可以快速达成一致的认知。

由此也可以看出，在这种网络中，只要事件能在全网中进行传播，即使不加入集中节点进行控制，最终网络中各实体针对一个事件 e 的信度也能达到很好的一致性。

对比图 4(a)~(b)可发现，在[0,1]均匀分布的初始信度下，信度合成前整个网络平均信度为 0.5，合成后，BA 无尺度网络平均信度为 0.32，而 NW 小世界网络平均信度为 0.51。由此我们可以得到：

结论 3：BA 无尺度网络中随机攻击一个网络实体，事件 e 的信度有降低的现象，这表明无尺度网络通过信度的合成有“澄清”虚假事件的能力，更难以攻击，相对于 NW 小世界网络，具有更强的抵抗能力。

这与 BA 无尺度网络在面对随机攻击时鲁棒性较强相吻合[14]。这也说明了这种鲁棒性不仅适用于物理域和信息域，在认知域上同样适用。

BA 无尺度网络对蓄意攻击具有高度的脆弱性[14]。为了检验在我们的仿真模型中是否也有类似的现象，我们对 step2 进行了修改，将随机的选择一个节点，变为选择节点度数最高的节点开始进行，并适当提高度数高的节点的信度。结果发现，其信度在合成后，具有明显的提升。如图 6 所示，平均信度由原来的 0.32 上升为 0.66。

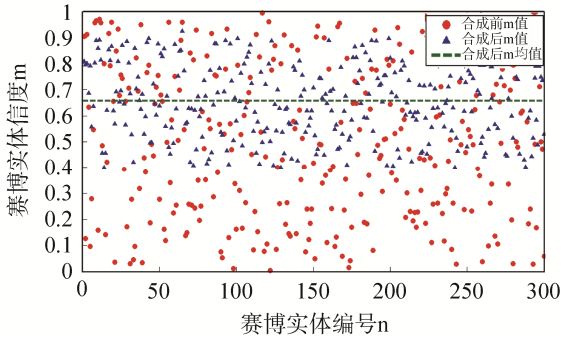


图 6 攻击关键节点 BA 无尺度网络信度演化

Fig. 6 BA scale-free network reliability evolution by attack critical nodes

由此我们可以看出，伪造事件对网络空间的影响，不仅与入口节点对事件的信度有关，还与入口节点自身的影响力有关，影响力大的节点作为入口节点，能够显著提升整个网络对事件的信度。节点的影响力大小与很多因素有关[15]，需要根据实际情况找出关键节点对伪造攻击加以防御。

5 结论

文章初步研究了面向认知域的网络攻击机理。这对于认识和防范刻意制造的“谣言”、“虚假信息”等网络攻击行为，提高网络空间安全具有现实意义，例如可以根据社会网络结构事先得到“虚假信息”攻击的影响范围，进一步分析虚假信息在群体中的信度分布和演化规律，为有效应对这类攻击提供技术指导。文章为了简化模型做了一些降低复杂性的假设。然而，由于面向感知共享的伪造攻击通常发生于认知域和社会域，网络实体的很多主观行为具有复杂性，这些复杂性可能会对结果产生影响。例如，本文对于每一个事件都假设在整个网络空间进行信度合成，这意味事件在全网络进行了传播。而一些传播动力学的研究发现，某些事件可能只会在网络的部分实体之间传播。因此，引入传播动力学以及实体行为模型对其进行更为深入的分析，是下一步还需要继续研究的一个方面。另外，通过收集典型的“谣言”引发的社会群体事件数据，分析“谣言”随时间在群体中的演化规律，来检验和修正基于 DS 证据理论的网络空间信度模型，也是下一步需要研究的内容。

参考文献：

[1] Scott Musman, Aaron Temin. Evaluating the Impact of Cyber Attacks on Missions[J]. The Journal of Defense Modeling and Simulation (S1548-5129), 2013: 25-36.

[2] 刘欣然. 网络攻击分类技术综述[J]. 通信学报, 2004, 25(7): 30-36.
LIU Xin-ran. Survey of network attack classification[J]. Journal on Communications | J Communs, 2004, 25(7): 30-36.

[3] David Silver, Aja Huang. Mastering The Game of Go with

https://dc-china-simulation.researchcommons.org/journal/vol30/iss9/4
DOI: 10.16182/j.issn1004731x.joss.201809004

Deep Neural Networks and Tree Search[J]. NATURE (S0028-0836), 2016, 529(1): 484-489.

[4] G Shafer. Comparing approximate reasoning and probabilistic reasoning using the Dempster-Shafer framework[J]. International Journal of Approximate Reasoning (S0888-613X), 2009, 50(5): 812-821.

[5] S Mckeever, J Ye, L Coyle, et al. Using Dempster-Shafer Theory of Evidence for Situation Inference[J]. Lecture Notes in Computer Science (S0302-9743), 2009, 5741(1): 149-161.

[6] Endsley M. Toward a Theory of Situation Awareness in Dynamic Systems[J]. Human Factors (S0018-7208), 1995, 37(1): 35-64.

[7] Endsley M R. Measurement of Situation Awareness in Dynamic Systems[J]. Human Factors (S0018-7208), 1995, 37(1): 65-84.

[8] Kevin Mepham, Panos Louvieris, Gheorghita Ghinea. Impact-Focused Cyber Incident Response[C]. 20th ICCRTS, 2015: 57.

[9] 史忠植. 人工智能[M]. 北京: 机械工业出版社, 2016: 123-131.
SHI Zhong-zhi. Artificial Intelligence[M]. Beijing: China Machine Press, 2016: 123-131.

[10] Yang J B, Xu D L. Evidential Reasoning Rule for Evidence Combination[J]. Artificial Intelligence (S0004-3702), 2013, 205(1): 1-29.

[11] Yong Deng. Generalized evidence theory[J]. Applied Intelligence, 2015, 43(3): 530-543.

[12] Barabási A-L. Scale-free networks: a decade and beyond[J]. Science (S0036-8075), 2009, 325(5939): 412-413.

[13] M E J Newman. Models of the Small World[J]. Journal of Statistical Physics (S0022-4715), 2000, 101(3): 819-841.

[14] Réka Albert, Hawoong Jeong, Albert-László Barabási. Error and attack tolerance of complex networks[J]. Nature, 2000, 406(1): 378-381.

[15] Jianxi Gao, Yang-Yu Liu, Raissa M D'Souza, et al. Target control of complex networks[J]. Nature Communications (S2041-1723), 2014, 5415(5): 1-8.

(上接第 3254 页)

[37] A Ridder. Importance sampling simulations of Monrovian reliability systems using cross-entropy[J]. Annals of Operations Research (S0254-5330), 2005, 143(6): 119-136.

[38] M de Konling, W Cai, B Sadigh, et al. Adaptive importance sampling Monte Carlo simulation of rare transition events[J]. Journal of Chemical Physics (S0021-9606), 2005, 122(7): 074103.

[39] F Cerou, P Del Moral, F Le Gland, et al. Genetic genealogical models in rare event analysis[J]. ALEA, Latin American Journal of Probability and Mathematical Statistics (S1980-0436), 2006, 1: 181-203.

[40] Zdravko I Botev, Pierre L'Ecuyer, Richard Simard, et al. Static Network Reliability Estimation under the Marshall-Olkin Copula[J]. ACM Transactions on Modeling and Computer Simulation (S1558-1195), 2016, 26(2): 14.

[41] Y Chen, P Diaconis, S Holmes, et al. Sequential Monte Carlo methods for statistical analysis of tables[J]. Journal of the American Statistical Association (S0162-1459), 2005, 100(469): 109-120.

[42] Graham Mauch Donovan. Rare Event Simulation for Lightwave Systems Using the Cross-Entropy Method[D]. PhD thesis, Northwestern University, Illinois, USA, 2008.

[43] W Sandmann. Discrete-time stochastic modeling and simulation of biochemical networks[J]. Computational Biology and Chmistry (S1476-9271), 2008, 32(4): 292-297.

[44] Hong Zhou, Yue Qiu, Yueqin Wu. An Early Warning System for Loan Risk Assessment Based on Rare Event Simulation[J]. AsiaSim, CCIS, 2007, 5: 85-94.