(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106341414 A
(43)申请公布日 2017.01.18

(21)申请号 201610866523.3

(22)申请日 2016.09.30

(71)申请人 重庆邮电大学
地址 400065 重庆市南岸区南山街道崇文路2号

(72)发明人 李方伟 王森 明月

(74)专利代理机构 北京一格知识产权代理事务所(普通合伙) 11316
代理人 滑春生

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/57(2013.01)

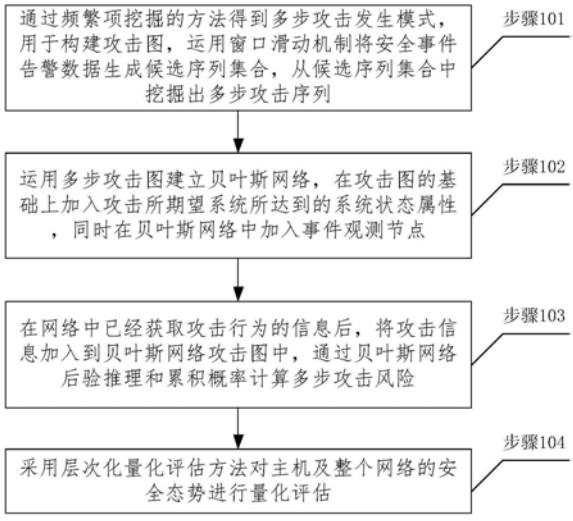
权利要求书3页 说明书10页 附图3页

(54)发明名称

一种基于贝叶斯网络的多步攻击安全态势评估方法

(57)摘要

本发明涉及网络安全态势评估方法，旨在提供一种基于贝叶斯网络的多步攻击安全态势评估方法，方法包括：首先通过关联分析挖掘多步攻击发生模式构建攻击图；然后根据多步攻击图建立贝叶斯网络，将攻击意愿、攻击成功概率、事件监测正确率定义为贝叶斯网络概率属性；结合事件监测，通过贝叶斯网络后验推理和累积概率计算多步攻击风险；采用层次化量化评估方法对主机及整个网络的安全态势进行量化评估；本发明解决了网络安全态势评估过程中缺乏关联性分析的问题，并把监测事件考虑到风险评估中，准确的建立网络安全态势评估模型，增强了本发明的有效性和实时性。



CN 106341414 A

1.一种基于贝叶斯网络的多步攻击安全态势评估方法,其特征在于,包括:

步骤A、通过频繁项挖掘得到多步攻击发生模式,用于构建攻击图,运用窗口滑动机制将安全事件告警数据生成候选序列集合,从候选序列集合中挖掘出多步攻击序列;

步骤B、运用多步攻击图建立贝叶斯网络,在攻击图的基础上加入攻击所期望系统所达到的系统状态属性,同时在贝叶斯网络中加入事件观测节点;

步骤C、将攻击信息加入到贝叶斯网络攻击图中,通过贝叶斯网络后验推理和累积概率计算多步攻击风险;

步骤D、采用层次化量化评估方法对主机及整个网络的安全态势进行量化评估。

2.根据权利要求1所述的网络安全态势评估方法,其特征在于,所述通过频繁项挖掘得到多步攻击发生模式,从候选序列集合中挖掘出多步攻击序列包括:

步骤A1,从网络中获取历史安全告警事件A_i($A_{i.time}$,$A_{i.s\text{-}ip}$,$A_{i.s\text{-}port}$,$A_{i.d\text{-}ip}$,$A_{i.d\text{-}port}$,s_{pre},s_{post},a_i,a_{item}),$A_{i.time}$为告警发生的时间;$A_{i.s\text{-}ip}$和$A_{i.d\text{-}ip}$为源IP和目的IP,$A_{i.s\text{-}port}$和$A_{i.d\text{-}port}$为源端口和目的端口,s_{pre}为攻击行为所需主机前提状态,s_{post}为攻击成功目的主机所处的状态,a_i为攻击类型标签,a_{item}报警序列号;

步骤A2,将历史攻击库中原子攻击按照时间属性排序,将排序后的原子攻击类型标签作为攻击序列集,设定窗口时间T_W,逐步向后滑动时间窗口,直至遍历完整个攻击序列集的所有元素,产生候选攻击序列集合AS=(as_1,as_2…as_n),as_n是候选攻击序列;

步骤A3,在候选攻击序列集中,基于挖掘关联规则的频繁项集Apriori算法挖掘最大频繁攻击序列集,然后将得到的频繁项序列集通过原子攻击报警序列号,根据时间属性对频繁项攻击序列再次排序,最后从频繁项序列集中找出最大频繁。

3.根据权利要求1所述的网络安全态势评估方法,其特征在于,所述运用多步攻击图建立贝叶斯网络,在攻击图的基础上加入攻击所期望系统所达到的系统状态属性,同时在贝叶斯网络中加入事件观测节点,包括:

步骤B1,定义贝叶斯网络为PAG=(N,E,P),N表示攻击图中的节点集,E表示节点之间的因果关系边集,P表示节点之间的条件概率集合;

其中,N=S∪A∪I表示攻击图中的节点集;S表示原子攻击所期望系统达到的目标状态集,每个多步攻击发起时系统所处的状态定义为系统初始状态s_0;A表示原子攻击集,A集合中的元素为通过频繁项挖掘所得到攻击图的每个原子攻击a_i;I表示原子攻击a_i的事件监测节点集,即任何一个攻击都有可能被监测设备正确识别;

因果关系边集E表示节点之间的因果关系;$E=E_{SA}\cup E_{AS}\cup E_{IA}$;其中,$E_{SA}$表示系统处于某一状态$s_i$条件下发生攻击$a_j$;$E_{AS}$表示某一原子攻击$a_j$发生后致使目标系统处于$s_i$状态;$E_{IA}$表示某一原子攻击$a_i$被入侵检测系统IDS识别,已确认$a_i$攻击已经发生;

P表示节点之间的条件概率表,$P=(P_{SA},P_{AS},P_{IA})$;其中,P_{SA}表示攻击目标处于状态s_i下发生攻击a_i的概率集合;P_{AS}表示原子攻击a_i成功使得系统处于目标状态s_i的概率集合;P_{IA}表示原子攻击a_i被正确识别的概率集合;

步骤B2,计算P_{AS}的量化公式:

$$P_{AS}=\frac{M}{e^{I}}\bullet PE$$

其中,M表示攻击行为属性与系统所处状态蕴含漏洞的匹配程度,如果攻击告警事件前

提条件中攻击目标的系统与实际网络中攻击目标操作系统进行匹配，如果匹配不成功，则M＝0.1，退出；否则继续匹配攻击行为端口与攻击目标系统开放端口是否匹配，如果不匹配，则M＝0.4，退出；否则判断该告警事件所针对的漏洞信息与目标系统漏洞是否匹配；如果不匹配，则M＝0.7，并退出匹配；如果匹配成功，则M＝1.0，I为攻击目标系统的安防措施，划分为5个可量化的数值等级，由弱到强分别为0.1、0.2、0.4、0.7和1.0，e^I为I的指数表达式；

PE为相应系统漏洞被攻击者利用的概率，根据通用安全漏洞评分系统CVSS通过脆弱性计分系统中的漏洞可利用的难易程度来量化；

步骤B3，计算P_{SA}：

$$P_{SA}=\begin{cases}0, \lambda \geq 1\\ 1-\lambda, 0<\lambda<1\\ 1, \lambda=0\end{cases}$$

其中，$\lambda=\frac{AC}{AP}$，为攻击的成本收益比，AC是攻击的成本，根据CVSS中攻击的复杂度量化生成的，攻击的收益AP＝L_j.weight-L_i.weight，L_i.weight为攻击a_i开始时目标系统的状态为s_i时的权限值，L_j.weight为攻击a_i结束时，目标系统的状态为s_j时的权限值。

4.根据权利要求1所述的网络安全态势评估方法，其特征在于，所述将攻击信息加入到贝叶斯网络攻击图中，通过贝叶斯网络后验推理和累积概率计算多步攻击风险，包括：

步骤C1，在贝叶斯网攻击图中，如果事件的发生已经被检测到，将这些事件作为证据节点集N_e，需要更新的节点集为发生在N_e之前的节点，记为N_u；通过贝叶斯公式计算后验概率在证据节点作用下，在证据节点集之前的节点发生的概率；对于$\forall N_i \in N_u$根据后验概率进行更新：

$$P(N_i=1|N_e=1)=\frac{P(N_e=1|N_i=1)\bullet P(N_i=1)}{P(N_e=1)}$$

$$P(N_i=1|N_e=0)=\frac{P(N_e=0|N_i=1)\bullet P(N_i=1)}{P(N_e=0)}$$

$P'(N_i=1)=P(N_i=1|N_e=1)\bullet P'(N_e=1)+P(N_i=1|N_e=0)\bullet P'(N_e=0)$

其中，1表示事件发生，0表示事件未发生，$P(N_e=1|N_i=1)$表示在原有的贝叶斯网中，在$\forall N_j \in N_e$的前一节点$\forall N_i \in N_u$发生的情况下，$\forall N_j \in N_e$发生的概率，$P(N_i=1|N_e=1)$表示在N_e发生的情况下，N_i发生的概率，$P(N_e=0|N_i=1)$表示在N_i发生的情况下，N_e不发生的概率，$P(N_i=1|N_e=0)$表示在N_e不发生的情况下，N_i发生的概率，$P(N_i)$和$P(N_e)$分别表示原贝叶斯网络攻击图中，节点N_i、N_e发生或不发生的概率，$P'(N_e=1)$、$P'(N_e=0)$分别表示更新后节点N_e发生和不发生的概率；

通过后验概率$P(N_i=1|N_e=1)$与证据节点N_e的概率$P'(N_e=1)=1$，得到在该证据下节点N_i的概率$P'(N_i=1)$，然后以N_i为证据，以同样的方法对它的前面的节点进行更新；

步骤C2，累积概率定义为在某一攻击检测到的情况下，结合攻击图，计算状态节点和攻击节点的累计概率，通过累积概率来描述多步攻击发生当前阶段的风险值。

5.根据权利要求1所述的网络安全态势评估方法，其特征在于，所述采用层次化量化评估方法对主机及整个网络的安全态势进行量化评估，包括：

步骤D1，在某一时刻当检测到某一攻击链中的某一原子攻击a_i发生，根据多步攻击发生模式可以得到当前时刻，针对该主机的发生的攻击为$a_1 \rightarrow a_2 \rightarrow \cdots \rightarrow a_i$，$a_1 \rightarrow a_2 \rightarrow \cdots \rightarrow a_i$为$a_1$、$a_2$……$a_i$对该主机依次攻击的多步攻击链；假设该攻击链完整的攻击步数为n，当前该攻击对主机的威胁值为：

$$Ts=ts \bullet CP(a_i) \bullet P_{(as)_i} \bullet e^{i/n}$$

其中，ts表述多步攻击威胁度，CP(a_i)为攻击a_i发生的累计概率；$P_{(as)_i}$描述了检测到该攻击发生可能攻击成功的概率，as为候选攻击序列；$e^{i/n}$为a_i处于整个攻击链中的阶段，描述一个多步攻击实施的程度；

步骤D2，主机资产重要性赋值，节点资产重要性M为：

$$M = Round(\sqrt{\frac{LC^2+LI^2+LA^2}{3}})$$

其中，LC、LI、LA表示安全属性值，分别是机密性属性值、完整性属性值和可用性属性值，根据等级从集合{1,2,4,6,8,10}中取值分别赋给所述三个属性值；

步骤D3，设某时间段内主机受到的多步攻击数量为s时，则该段时间主机ℓ受到攻击的威胁值：

$$TD_\ell = M \bullet \sum_{i=1}^{s} Ts_i$$

其中Ts_i表示攻击a_i对主机的威胁值；

步骤D4，系统态势量化，则整个网络系统的威胁值RN为：

$$RN = \sum_{\ell=1}^{l} TD_\ell \bullet w_\ell$$

其中，l为网络中主机数量，w_ℓ为主机的权重值。

一种基于贝叶斯网络的多步攻击安全态势评估方法

技术领域

[0001] 本发明涉及网络安全评估方法，特别涉及一种基于贝叶斯网络的多步攻击安全态势评估方法。

背景技术

[0002] 随着我国互联网市场规模和用户量高速增长，所面临的网络安全问题也相伴而生。这使得互联网在惠及广大群众的同时受到信息盗窃、故障、偶发事件、病毒等多方面的挑战，网络安全性、可用性问题越来越突出。因此，亟需一种新的安全技术能够处理大规模网络日常数据并且形成针对性的防护策略，来提高网络安全性能，网络安全态势感知研究应运而生。

[0003] 网络安全态势感知是一种主动的安全防御机制。它将从安全设备所采取的多源异构数据，通过数据融合技术进行规范化整合，然后从融合后的数据中获取影响网络正常运行的安全态势要素。采用合理准确的态势评估方法对所获取的安全态势要素进行评估，得到当前网络安全状态。同时根据当前安全态势预测未来网络安全趋势。网络安全态势感知协助网络管理人员更加直观的理解网络所面临的安全威胁，针对性的采取响应策略。同时掌握网络安全趋势和可能会出现的网络攻击行为，为管理员制定有效的预防策略提供可靠的依据。

[0004] 目前，网络安全态势感知的研究还处于初步阶段，Stephen等研发了一个集成现有网络安全技术的系统架构，用以提供大规模复杂网络的实时感知功能，并利用可视化方式直观反映了当前网络的安全状态。陈秀真提从出漏洞、主机、网络系统三个方面对网络安全进行评估的层次化模型，该模型采取从下往上，先局部后整体的思路，从安全威胁，主机以及服务的权重对网络系统、主机、服务和漏洞评估威胁态势。罗智勇等人为解决入侵意图难以被发现的问题，探索了一种入侵意图自动识别系统，在该系统中采用动态攻击图技术，结合资产、脆弱性等安全特征，以最小关键点集生成算法来搜寻网络中的重要主机，实现动态网络评估的目的。刘效武等人针对态势感知中多源数据信息融合的问题，在引用D-S证据理论的基础上，利用粒子群优化算法对不同数据源信任度权值重新分配，同时，采用离散化方式对正态分布的数据进行处理，提出了具有自适应能力的威胁因子获取方法，在此基础上评估网络威胁。

发明内容

[0005] 本发明的目的是提供一种基于贝叶斯网络的多步攻击安全态势评估方法，来解决多步攻击的威胁评估，缺乏多步骤之间关联性的问题，并把监测事件考虑到风险评估中，准确的建立网络安全态势评估模型，增强了本发明的有效性和实时性。

[0006] 针对现有技术的不足，本发明提供一种基于贝叶斯网络的多步攻击安全态势评估方法，具体包括下述步骤：

[0007] 步骤A、通过频繁项挖掘的方法得到多步攻击发生模式，用于构建攻击图，运用窗

口滑动机制将安全事件告警数据生成候选序列集合，从候选序列集合中挖掘出多步攻击序列。

[0008] 步骤B、运用多步攻击图建立贝叶斯网络，在攻击图的基础上加入攻击所期望系统所达到的系统状态属性，同时在贝叶斯网络中加入事件观测节点。

[0009] 步骤C、在网络中已经获取攻击行为的信息后，将攻击信息加入到贝叶斯网络攻击图中，通过贝叶斯网络后验推理和累积概率计算多步攻击风险。

[0010] 步骤D、采用层次化量化评估方法对主机及整个网络的安全态势进行量化评估。

[0011] 优选地，所述步骤A包括如下步骤：

[0012] 步骤A1，从网络中获取历史安全告警事件A_i($A_{i.time}$,$A_{i.s\text{-}ip}$,$A_{i.s\text{-}port}$,$A_{i.d\text{-}ip}$,$A_{i.d\text{-}port}$,s_{pre},s_{post},a_i,a_{item})，A_i()表示安全告警事件集合，$A_{i.time}$为告警发生的时间。$A_{i.s\text{-}ip}$和$A_{i.d\text{-}ip}$为源IP和目的IP。$A_{i.s\text{-}port}$和$A_{i.d\text{-}port}$为源端口和目的端口。s_{pre}为攻击行为所需主机前提状态。s_{post}为攻击成功目的主机所处的状态。a_i为攻击类型标签，a_{item}报警序列号。

[0013] 步骤A2，将历史攻击库中原子攻击按照时间属性排序，将排序后的原子攻击类型标签作为攻击序列集。设定窗口时间T_W，逐步向后滑动时间窗口，直至遍历完整个攻击序列集的所有元素，产生候选攻击序列集合AS＝(as_1,as_2…as_n)，as_n是候选攻击序列。

[0014] 步骤A3，在候选攻击序列集中，基于挖掘关联规则的频繁项集Apriori算法挖掘最大频繁攻击序列集。然后将得到的频繁项序列集通过原子攻击报警序列号，根据时间属性对频繁项攻击序列再次排序。最后从频繁项序列集中找出最大频繁。

[0015] 优选地，所述步骤B包括如下步骤：

[0016] 步骤B1，定义贝叶斯网络为PAG＝(N,E,P)。N表示攻击图中的节点集，E表示节点之间的因果关系边集，P表示节点之间的条件概率集合。

[0017] 其中，N＝S∪A∪I表示攻击图中的节点集。S表示原子攻击所期望系统达到的目标状态集，每个多步攻击发起时系统所处的状态定义为系统初始状态s_0。A表示原子攻击集。A集合中的元素为通过频繁项挖掘所得到攻击图的每个原子攻击a_i。I表示原子攻击a_i的事件监测节点集，即任何一个攻击都有可能被监测设备正确识别。

[0018] 有向边集E表示节点之间的因果关系。E＝E_{SA}∪E_{AS}∪E_{IA}。其中，E_{SA}表示系统处于某一状态s_i条件下发生攻击a_j。E_{AS}表示某一原子攻击a_j发生后致使目标系统处于s_i状态。E_{IA}表示某一原子攻击a_i被入侵检测系统IDS系统识别，已确认a_i攻击已经发生。

[0019] P表示节点之间的条件概率表，P＝(P_{SA},P_{AS},P_{IA})。其中，P_{SA}表示攻击目标处于状态s_i下发生攻击a_i的概率$P_{(sa)_{ij}}$集合。同样，P_{AS}表示原子攻击a_i成功使得系统处于目标状态s_i的概率$P_{(as)_{it}}$集合。P_{IA}表示原子攻击a_i被正确识别的概率P_{Ia_i}的集合。

[0020] 步骤B2，计算攻击成功概率P_{AS}的量化公式：

[0021] $$P_{AS}=\frac{M}{e^{I}}\bullet PE$$

[0022] 其中，M表示攻击行为属性与系统所处状态蕴含漏洞的匹配程度，如果攻击告警事件前提条件中攻击目标的系统与实际网络中攻击目标操作系统进行匹配，如果匹配不成功，则M＝0.1，退出。否则继续匹配攻击行为端口与攻击目标系统开放端口是否匹配，如果不匹配，则M＝0.4，退出。否则判断该告警事件所针对的漏洞信息与目标系统漏洞是否匹

配。如果不匹配，则M＝0.7，并退出匹配。如果匹配成功，则M＝1.0。I为攻击目标系统的安防措施，划分为5个可量化的数值等级，由弱到强分别为0.1、0.2、0.4、0.7和1.0，e^I为I的指数表达式。

[0023] PE为相应系统漏洞被攻击者利用的概率，通过通用安全漏洞评估系统(Common Vulnerability Scoring System，CVSS)中的漏洞可利用的难易程度来量化。CVSS，是美国国家基础设施顾问委员会(NIAC)实施的一个项目，该项目旨在建立一个计算机系统安全漏洞评估框架，使用统一的语言对计算机系统内所有安全漏洞的严重性、整个网络的脆弱性进行评估，为所有安全漏洞的严重程度提供了一个量化评估值。

[0024] 步骤B3，计算系统处于某种状态下发起攻击的概率P_{SA}：

[0025] $$P_{SA}=\begin{cases}0, \lambda \geq 1\\ 1-\lambda, 0<\lambda<1\\ 1, \lambda=0\end{cases}$$

[0026] 其中，$\lambda=\frac{AC}{AP}$，为攻击的成本收益比。CVSS对网络脆弱性的评估主要包括：基本评估、时效性评估、环境评估。其中基本评估中有一项就是攻击复杂度(AC)。AC是攻击的成本，根据CVSS中攻击的复杂度量化生成的，攻击的收益AP＝L_j.weight-L_i.weight，L_i.weight为攻击a_i开始时目标系统的状态为s_i时的权限值，L_j.weight为攻击a_i结束时，目标系统的状态为s_j时的权限值。

[0027] 优选地，所述步骤C包括如下步骤：

[0028] 步骤C1，在贝叶斯网攻击图中，如果事件的发生已经被检测到，将这些事件作为证据节点集N_e，需要更新的节点集为发生在N_e之前的节点，记为N_u。通过贝叶斯公式计算后验概率在证据节点作用下，在证据节点集之前的节点发生的概率。对于$\forall N_i \in N_u$根据后验概率进行更新。

[0029] $$P(N_i=1|N_e=1)=\frac{P(N_e=1|N_i=1)\bullet P(N_i=1)}{P(N_e=1)}$$

[0030] $$P(N_i=1|N_e=0)=\frac{P(N_e=0|N_i=1)\bullet P(N_i=1)}{P(N_e=0)}$$

[0031] $P'(N_i=1)=P(N_i=1|N_e=1)\cdot P'(N_e=1)+P(N_i=1|N_e=0)\cdot P'(N_e=0)$

[0032] 其中，1表示事件发生，0表示事件未发生，$P(N_e=1|N_i=1)$表示在原有的贝叶斯网中，在$\forall N_j \in N_e$的前一节点$\forall N_i \in N_u$发生的情况下，$\forall N_j \in N_e$发生的概率，$P(N_i=1|N_e=1)$表示在N_e发生的情况下，N_i发生的概率，$P(N_e=0|N_i=1)$表示在N_i发生的情况下，N_e不发生的概率，$P(N_i=1|N_e=0)$表示在N_e不发生的情况下，N_i发生的概率，$P(N_i)$和$P(N_e)$分别表示原贝叶斯网络攻击图中，节点N_i发生的概率和节点N_e的发生概率，$P'(N_e=1)$、$P'(N_e=0)$分别表示更新后节点N_e发生和不发生的概率。

[0033] 通过后验概率$P(N_i=1|N_e=1)$与证据节点N_e的概率$P'(N_e=1)=1$，得到在该证据下节点N_i的概率$P'(N_i=1)$，然后以N_i为证据，以同样的方法对它的前面的节点进行更新。

[0034] 步骤C2，累积概率定义为在某一攻击检测到的情况下，结合攻击图，计算状态节点和攻击节点的累计概率，通过累积概率来描述多步攻击发生当前阶段的风险值。

[0035] 优选地，所述步骤D包括如下步骤：

[0036] 步骤D1，在某一时刻当检测到某一攻击链中的某一原子攻击a_i发生，根据多步攻击发生模式可以得到当前时刻，针对该主机的发生的攻击为$a_1 \rightarrow a_2 \rightarrow \cdots \rightarrow a_i$（$a_1 \rightarrow a_2 \rightarrow \cdots \rightarrow a_i$为$a_1$、$a_2$……$a_i$对该主机依次攻击的多步攻击链，即表示$a_1$攻击该主机，然后$a_2$攻击该主机，然后$a_3$攻击该主机，……）。假设该攻击链完整的攻击步数为n。当前该攻击对主机的威胁值为：

[0037] $$Ts=ts \bullet CP(a_i) \bullet P_{(as)_i} \bullet e^{i/n}$$

[0038] 其中，ts表述多步攻击攻击威胁度，CP(a_i)为攻击a_i发生的累计概率；$P_{(as)_i}$描述了检测到该攻击发生可能攻击成功的概率，as为候选攻击序列。$e^{i/n}$为a_i处于整个攻击链中的阶段，描述一个多步攻击实施的程度。

[0039] 步骤D2，主机资产重要性赋值，主机资产重要性主要是从机密性(LC)，完整性(LI)，可用性(LA)三个安全属性来描述主机资产对安全性的要求。根据等级从集合{1,2,4,6,8,10}中取值分别赋给所述三个属性值。节点资产重要性M为：

[0040] $$M = Round(\sqrt{\frac{LC^2+LI^2+LA^2}{3}})$$

[0041] 步骤D3，设某时间段内主机受到的多步攻击数量为s时，则该段时间主机ℓ受到攻击的威胁值：

[0042] $$TD_\ell = M \bullet \sum_{i=1}^{s} Ts_i$$

[0043] Ts_i表示攻击a_i对主机的威胁值；

[0044] 步骤D4，系统态势量化，假设网络中有l台主机，主机的权重值为w_ℓ，则整个网络系统的威胁值RN为：

[0045] $$RN = \sum_{\ell=1}^{l} TD_\ell \bullet w_\ell$$

[0046] 根据主机在网络中所担负的作用对主机的权重赋值。

[0047] 与现有技术比，本发明达到的有益效果是：

[0048] 本发明提供了一种基于贝叶斯网络的多步攻击安全态势评估方法，采用频繁项挖掘的方法得到多步攻击发生模式，根据多步攻击发生模式，建立了基于攻击图的贝叶斯网络。在实时攻击监测的条件下，通过贝叶斯网络后验推理，得到多步攻击中每步攻击发生的概率。通过计算累积概率描述多步攻击发生到当前阶段的风险；在量化评估中，根据资产损失最大评估多步攻击不同阶段的威胁度。通过层次化量化评估模型，对网络进行安全态势量化评估。本文方法针对多步攻击进行有效的、实时的评估，能够为管理员分析网络实时安全态势提供了依据。

附图说明

[0049] 图1是本发明提供的网络安全态势评估方法的流程图；

[0050] 图2是基于窗口滑动的候选序列生成过程图；

[0051] 图3是本发明提供的层次化态势评估模型简略图；

[0052] 图4是本发明攻击威胁度仿真对比图；

[0053] 图5是本发明网络系统的安全态势评估仿真对比图。

具体实施方式

[0054] 下面结合附图对本发明的具体实施方式作进一步的详细说明。

[0055] 图1是本发明提供的网络安全态势评估方法的流程图，包括下述步骤：

[0056] 步骤101，通过频繁项挖掘的方法得到多步攻击发生模式，用于构建攻击图，运用窗口滑动机制将安全事件告警数据生成候选序列集合，从候选序列集合中挖掘出多步攻击序列。

[0057] 步骤102，运用多步攻击图建立贝叶斯网络，在攻击图的基础上加入攻击所期望系统所达到的系统状态属性，同时在贝叶斯网络中加入事件观测节点。

[0058] 步骤103，在网络中已经获取攻击行为的信息后，将攻击信息加入到贝叶斯网络攻击图中，通过贝叶斯网络后验推理和累积概率计算多步攻击风险。

[0059] 步骤104，采用层次化量化评估方法对主机及整个网络的安全态势进行量化评估。

[0060] 根据本发明，其中，步骤101进一步包括以下步骤：

[0061] 步骤101-1，历史安全告警事件A_i($A_{i.time}$，$A_{i.s\text{-}ip}$，$A_{i.s\text{-}port}$，$A_{i.d\text{-}ip}$，$A_{i.d\text{-}port}$，s_{pre}，s_{post}，a_i，a_{item})，$A_{i.time}$为告警发生的时间。$A_{i.s\text{-}ip}$和$A_{i.d\text{-}ip}$为源IP和目的IP。$A_{i.s\text{-}port}$和$A_{i.d\text{-}port}$为源端口和目的端口。s_{pre}为攻击行为所需主机前提状态。s_{post}为攻击成功目的主机所处的状态。a_i为攻击类型标签，a_{item}报警序列号。

[0062] 步骤101-2，将历史攻击库中原子攻击按照时间属性排序，将排序后的原子攻击类型标签作为攻击序列集。基于窗口滑动的候选序列生成过程如图2，设定窗口时间T_W，逐步向后滑动时间窗口，同处于一个窗口的攻击属于一个攻击候选序列，一个多步攻击的完整步骤包含在候选攻击序列中。

[0063] 随着窗口每一步后移都会产生一个候选攻击序列，直至遍历完整个攻击序列集的所有元素，产生候选攻击序列集合AS＝(as_1，as_2…as_n)。

[0064] 步骤101-3，在候选攻击序列集中，基于Apriori算法挖掘最大频繁攻击序列集，多步攻击发掘算法通过扫描历史攻击库和攻击序列，挖掘最大频繁项L_k，与最小支持度进行比较，如果是大于最小支持度，进行Max-L＝Max-L∪L_k，刚开始Max-L为空集，循环过程，直到最后小于最小支持度时，得到最终的Max-L。

[0065] 在Apriori算法中，序列包含，候选攻击序列as_i和as_j，如果$as_i \subseteq as_j$，则as_i中的元素包含在as_j中。但是通过窗口滑动所产生的获选攻击序列中，相邻的候选攻击序列中的元素会重复的出现，那么某一个序列可能会重复包含。根据窗口滑动所产生候选攻击序列的特点，定义两个序列包含，如$as_i \subseteq as_j$，在原有包含的定义基础上，限制序列as_i和序列as_j的第一个元素必须是相同的，as_i其余的元素都在as_j中，则称$as_i \subseteq as_j$。

[0066] 攻击序列支持度，针对某一攻击目标的多步攻击中包含有m个不同的攻击类型，有序的攻击行为所构成的序列称为攻击序列。如果候选攻击序列as_i包含攻击序列X，则称as_i支持X。候选攻击序列集AS中包含攻击序列X的候选攻击序列所占的百分比称为攻击序列的支持度。

[0067] 频繁项序列。攻击序列的支持度大于人为设定的最小支持度，该序列则称为频繁

项序列。根据Apriori算法性质，如果某一攻击序列为频繁项序列，那么该序列的子集也属于频繁项序列。

[0068] 最大攻击序列。如果某一攻击序列没有被其他攻击序列所包含，则该序列为最大攻击序列。记Max-L为最大攻击序列集。

[0069] k-频繁项。如果某一频繁项序列包含有k个元素，则称其为k-频繁项，记为L_k。通过L_k所产生的备选频繁项记为C_{k+1}。

[0070] 由于通过窗口滑动机制所产生的候选攻击序列，致使一些元素会在不同的候选攻击序列中重复出现，因此在产生L_1时，通过遍历历史攻击库，得到攻击库中的攻击行为a_i在攻击库中出现的比例，将此定义为1-项集的支持度，通过人为设定的最小支持度，对1-项集进行筛选，去除低于最小支持度的项目，得到频繁项目集L_1。

[0071] 得到的频繁项序列集中的原子攻击是无序的，然后通过原子攻击报警序列号，根据时间属性对频繁项攻击序列再次排序。最后从频繁项序列集中找出最大频繁攻击序列集。

[0072] 根据本发明，其中，步骤102进一步包括以下步骤：

[0073] 步骤102-1，定义贝叶斯网络为PAG＝(N,E,P)。N表示攻击图中的节点集，E表示节点之间的因果关系边集，P表示节点之间的条件概率集合。

[0074] 节点集N＝S∪A∪I。其中，S表示原子攻击所期望系统达到的目标状态集，每个多步攻击发起时系统所处的状态定义为系统初始状态s_0。A表示原子攻击集。A集合中的元素为通过频繁项挖掘所得到攻击图的每个原子攻击a_i。I表示原子攻击a_i的事件监测节点集，即任何一个攻击都有可能被监测设备正确识别。

[0075] 有向边集E表示节点之间的因果关系。$E＝E_{SA}∪E_{AS}∪E_{IA}$。其中，E_{SA}表示系统处于某一状态s_i条件下发生攻击a_j。E_{AS}表示某一原子攻击a_j发生后致使目标系统处于s_i状态。E_{IA}表示某一原子攻击a_i被IDS系统识别，已确认a_i攻击已经发生。

[0076] P表示节点之间的条件概率表，$P＝(P_{SA},P_{AS},P_{IA})$。其中，P_{SA}表示攻击目标处于状态s_i下发生攻击a_i的概率$P_{(sa)_{ij}}$集合。同样，P_{AS}表示原子攻击a_i成功使得系统处于目标状态s_i的概率$P_{(as)_{ii}}$集合。P_{IA}表示原子攻击a_i被正确识别的概率P_{Ia_r}的集合。

[0077] 步骤102-2，为了更加客观的反应攻击成功的概率与其系统的客观状态的关系，提出攻击成功概率P_{AS}的量化公式：

[0078] $$P_{AS}=\frac{M}{e^{I}}\bullet PE$$

[0079] 其中，M表示攻击行为属性与系统所处状态蕴含漏洞的匹配程度。匹配度M量化，提取告警事件的时间、攻击类型、目的IP、端口等相关属性，与原子攻击所依赖的前提条件库和漏洞信息进行匹配。

[0080] 如果攻击告警事件前提条件中攻击目标的系统与实际网络中攻击目标操作系统进行匹配，如果匹配不成功，则M＝0.1，退出。否则继续匹配攻击行为端口与攻击目标系统开放端口是否匹配，如果不匹配，则M＝0.4，退出。否则判断该告警事件所针对的漏洞信息与目标系统漏洞是否匹配。如果不匹配，则M＝0.7，并退出匹配。如果匹配成功，则M＝1.0。

[0081] I为攻击目标系统的安防措施对安防措施程度划分为5个等级，并进行数值量化。PE为相应系统漏洞被攻击者利用的概率。漏洞利用率PE量化，通过通用安全漏洞评估系统

(Common Vulnerability Scoring System,CVSS)中的漏洞可利用的难易程度来量化。CVSS,是美国国家基础设施顾问委员会(NIAC)实施的一个项目,该项目旨在建立一个计算机系统安全漏洞评估框架,使用统一的语言对计算机系统内所有安全漏洞的严重性、整个网络的脆弱性进行评估,为所有安全漏洞的严重程度提供了一个量化评估值。

[0082] 步骤102-3,某个原子攻击是否会发生,依据于攻击的成本收益比,$\lambda=\frac{AC}{AP}$,则P_{SA}量化方法为:

[0083] $$P_{SA}=\begin{cases}0, \lambda\geq 1\\ 1-\lambda, 0<\lambda<1\\ 1, \lambda=0\end{cases}$$

[0084] 根据上述公式,当λ≥1时,攻击成本要大于攻击意愿,攻击发生的可能性非常小。当λ=0时,攻击成本几乎为0,攻击在这种情况下发起攻击的概率非常大。

[0085] P_{SA}是系统处于某种状态下发起攻击的概率。攻击这在发起一个攻击行为时,考虑攻击所付出的代价,一般以攻击的复杂度量化,复杂度越高,攻击就要付出较高的攻击成本。CVSS对网络脆弱性的评估主要包括:基本评估、时效性评估、环境评估。其中基本评估中有一项就是攻击复杂度(AC)。根据CVSS中攻击的复杂度生成量化的AC。

[0086] 同时还要考虑攻击收益,攻击期望目标系统所处状态决定攻击收益,攻击获得的权限越高,其攻击收益越大。某一攻击a_i使得目标系统的状态从s_i转移到s_j状态时所获得权限从L_i提升到L_j。攻击的收益AP=L_j.weight-L_i.weight(L_i.weight、L_j.weight分别为权限L_i和L_j所占的权重)。对攻击的所要达到的最终状态进行划分,对应5个不同的等级。

[0087] 根据本发明,其中,步骤103进一步包括以下步骤:

[0088] 步骤103-1,在贝叶斯网攻击图中,如果事件的发生已经被检测到,将这些事件作为证据节点集N_e,N=S∪A∪I,需要更新的节点集为发生在N_e之前的节点,记为N_u。通过贝叶斯公式计算后验概率计算在证据节点作用下,在证据之前的节点发生的概率。对于$\forall N_i\in N_u$根据后验概率进行更新。

[0089] $$P(N_i=1\mid N_e=1)=\frac{P(N_e=1\mid N_i=1)\bullet P(N_i=1)}{P(N_e=1)}$$

[0090] $$P(N_i=1\mid N_e=0)=\frac{P(N_e=0\mid N_i=1)\bullet P(N_i=1)}{P(N_e=0)}$$

[0091] $P'(N_i=1)=P(N_i=1\mid N_e=1)\cdot P'(N_e=1)+P(N_i=1\mid N_e=0)\cdot P'(N_e=0)$

[0092] 其中,1表示事件发生,0表示事件未发生,$P(N_e=1\mid N_i=1)$表示在原有的贝叶斯网中,在$\forall N_j\in N_e$的前一节点$\forall N_i\in N_u$发生的情况下,$\forall N_j\in N_e$发生的概率,$P(N_i)$和$P(N_e)$分别表示原贝叶斯网络攻击图中,节点N_i发生的概率和节点N_e的发生概率。

[0093] 通过后验概率$P(N_i=1\mid N_e=1)$与证据节点N_e的概率$P'(N_e=1)=1$,得到在该证据下节点N_i的概率$P'(N_i=1)$,然后以N_i为证据,以同样的方法对它的前面的节点进行更新。

[0094] 步骤103-2,累积概率定义为在某一攻击检测到的情况下,结合攻击图,计算状态节点和攻击节点的累积概率,通过累积概率来描述多步攻击发生当前阶段的风险值。根据步骤103-1后验概率更新节点。累积概率CP定义如下。

[0095] (1)如果一件攻击行为被检测到,确定事件已经发生,则$CP(I_j)=1$;

[0096] (2)多步攻击第一步攻击发生的前提状态记为s_0,认为$CP(s_0)=P(s_0)$,记$Pre(s_i)$为s_i的前一节点,前一节点状态的累积概率计算公式如下所示:

[0097] $$CP(s_i)=\oplus(Pre(s_i)),i\neq 0$$

[0098] (3)对于攻击的累积概率为$CP(a_i)$,如果a_i攻击行为没有被检测到,需要结合步骤103-1的后验概率更新节点,则其累积概率计算方法如下:

[0099] $$CP(a_i)=P_{(Pre(a_i))}\mathrm{U}(Pre(Pre(a_i)))$$

[0100] 如果a_i攻击行为被检测到,则其累积概率计算方法如下:

[0101] $$CP(a_i)=\oplus(Pre(a_i),I_i)$$

[0102] 其中,

[0103] $$\oplus(Pre(a_i),I_i)=CP(s_{i\text{-}1})P_{(sa)_{i-1,i}}+CP(I_i)P_{Ia_i}-CP(s_i)P_{(sa)_{i-1,i}}CP(I_i)P_{Ia_i}$$

[0104] $U(Pre(a_i))=CP(Pre(a_i))$

[0105] $$\oplus(Pre(s_i))=CP(Pre(s_i))P_{(as)_{i,i}}$$

[0106] 以上式中,$P_{(sa)_{i-1,i}}$为攻击目标处于状态s_i下发生攻击a_i的概率,$P_{(sa)_{i-1,i}}$的集合为步骤102中的P_{SA},$P_{(as)_{ii}}$为原子攻击a_i成功使得系统处于目标状态s_i的概率,$P_{(as)_{ii}}$的集合为步骤102中的P_{AS},P_{Ia_i}为攻击a_i被正确识别的概率,P_{Ia_i}的集合为步骤102中的P_{IA}。

[0107] 图3是本发明的层次化态势评估模型。根据本发明,步骤104即所述态势评估进一步包括以下步骤:

[0108] 通过贝叶斯推理多步攻击可达概率的基础上,采用层次化评估模型,根据攻击发起概率、攻击成功概率、事件监测正确率获取攻击风险度,从攻击风险度、单步原子攻击威胁量化攻击链威胁值。然后依据完整性、机密性、可用性三个方面评估主机所已拥有的资产价值来量化主机的重要性。从主机的资产价值和当前所面临的攻击链威胁值量化当前主机的威胁态势值;根据整个网络系统中所有主机所面临的威胁态势值和主机在整个网络中权重量化整个网络系统的态势值。

[0109] 步骤104-1,在某一时刻当检测到某一攻击链中的某一原子攻击a_i发生,根据多步攻击发生模式可以得到当前时刻,针对该主机的发生的攻击为$a_1\rightarrow a_2\rightarrow\cdots\rightarrow a_i$。假设该攻击链完整的攻击步数为n。当前该攻击对主机的威胁值为:

[0110] $$Ts=ts\bullet CP(a_i)\bullet P_{(as)_i}\bullet e^{i/n}$$

[0111] 其中,ts表述多步攻击攻击威胁度,$CP(a_i)$为攻击a_i发生的累计概率,刻画达到当前攻击的风险度。$P_{(as)_i}$描述了检测到该攻击发生可能攻击成功的概率。$e^{i/n}$为a_i处于整个攻击链中的阶段,描述一个多步攻击实施的程度,能够表达随着攻击逐步发生,其对目标威胁度增长越快。

[0112] 根据CVSS评估标准,某一攻击对主机资产值所造成的损失值为该原子攻击的威胁值,以此对原子攻击威胁进行量化分析。对于多步攻击的评估,按每步攻击对主机机密性、完整性、可用性所造成的损失的最大值作为多步攻击的所造成的损失。多步攻击ts量化如下所示:

[0113] $$ts = \log_2 \frac{(2^{C_{max}} + 2^{I_{max}} + 2^{A_{max}})}{3}$$

[0114] 其中C,I,A分别表示攻击对主机资产的机密性,完整性,可用性造成的损失。

[0115] 在多步攻击$a_1 \rightarrow a_2 \rightarrow \cdots \rightarrow a_i$中每步攻击对主机资产所造成的损失分别为$C_i$、$I_i$、$A_i$。而整个多步攻击对资产造成损失$C_{max}=max(C_i)$,$I_{max}=max(I_i)$,$A_{max}=max(A_i)$。

[0116] 步骤104-2,主机资产重要性赋值,主机资产重要性主要是从机密性(LC),完整性(LI),可用性(LA)三个安全属性来描述主机资产对安全性的要求。根据等级分别赋值三个属性值(1,2,4,6,8,10)。节点资产重要性M为:

[0117] $$M = Round(\sqrt{\frac{LC^2+LI^2+LA^2}{3}})$$

[0118] 步骤104-3,设某时间段内主机受到的多步攻击数量为s时,则该段时间主机ℓ受到攻击的威胁值:

[0119] $$TD_\ell = M \bullet \sum_{i=1}^{s} Ts_i$$

[0120] 步骤104-4,系统态势量化,假设网络中有l台主机,主机的权重值为w_ℓ,则整个网络系统的威胁值RN为:

[0121] $$RN = \sum_{\ell=1}^{l} TD_\ell \bullet w_\ell$$

[0122] 根据主机在网络中所担负的作用对主机的权重赋值。

[0123] 图4是本发明在情况一、情况二、B-AG和T-SA四种方法下攻击威胁度仿真对比图,其中B-AG是通过引入攻击证据与CVSS评分系统,提出了一种面向脆弱点的网络安全量化评估方法,T-SA是一种基于时空关联分析的网络实时威胁识别与量化评估方法。在针对威胁度量化中,通过对多步攻击每一原子攻击对资产所造成的损失进行了关联分析,将各个原子攻击对资产造成的损失度的最大值作为多步攻击的威胁值。同时还考虑了检测事件,在此处阐述两种极限的情况下的多步攻击威胁度。情况一:某一多步攻击发生到某一步骤时,事件监测设备检测到该攻击行为,而之前的攻击行为都未检测到。情况二:某一多步攻击发生的每一个步骤都被监测设备检测到。B-AG基于攻击图的安全态势评估中,对于多步攻击威胁值为多步攻击进行到当前阶段的原子攻击威胁。而T-SA中,多步攻击发生到当前阶段威胁值为多步攻击中所有发生了的攻击的威胁值累加。

[0124] 图4中可以看出,B-AG对每个阶段攻击威胁值的评估,不能够很好的描述出随着多步攻击的不断深入,攻击威胁越大。而T-SA的威胁评估方法,虽然能够较好的反映出随着攻击阶段的深入,攻击威胁值也随之增加的趋势,但是累加的方法在评估过程,重复计算了资产的损失,导致攻击威胁急剧上升。本发明方法通过关联多步攻击对资产造成的损失,对攻击威胁值的评估更加客观同时还很好刻画了随着攻击阶段的增加,攻击威胁值增加越快的趋势。

[0125] 图5是本发明网络系统的安全态势评估仿真对比图,从图中可以看出,B-AG的评估所得的态势值太低,这会导致漏警现象的发生,同时在在第7时间段到第8时间段中,攻击接近完成阶段,而网络安全态势值的增长并不太明显。这会使得管理员产生错误的判断,不能做出有效的应对措施。而T-SA,由于采用威胁值得累加,如果攻击步骤较多时,可能在攻击

的中间阶段会出现态势值较高的现象，如果此时的态势值高于设置的某一临界值，会不断的产生报警，从而导致误警较多。本文方法在监测事件的条件下，根据攻击图，得到多步攻击发生到当前阶段的风险值，并对不同阶段的攻击威胁值进行了综合评估，从上图中本文方法可以直观的显示整个网络的受到攻击的状况，从而可以给管理员提供依据来制定安防策略。

[0126] 最后应当说明的是：参照上述实施例对本发明进行了详细的说明，本发明并非限制于这里所描述的实施例，任何对本发明的技术方案的修改或者等同替换，都未脱离本发明技术方案的范围，均在申请待批的本发明的权利要求保护范围之内。

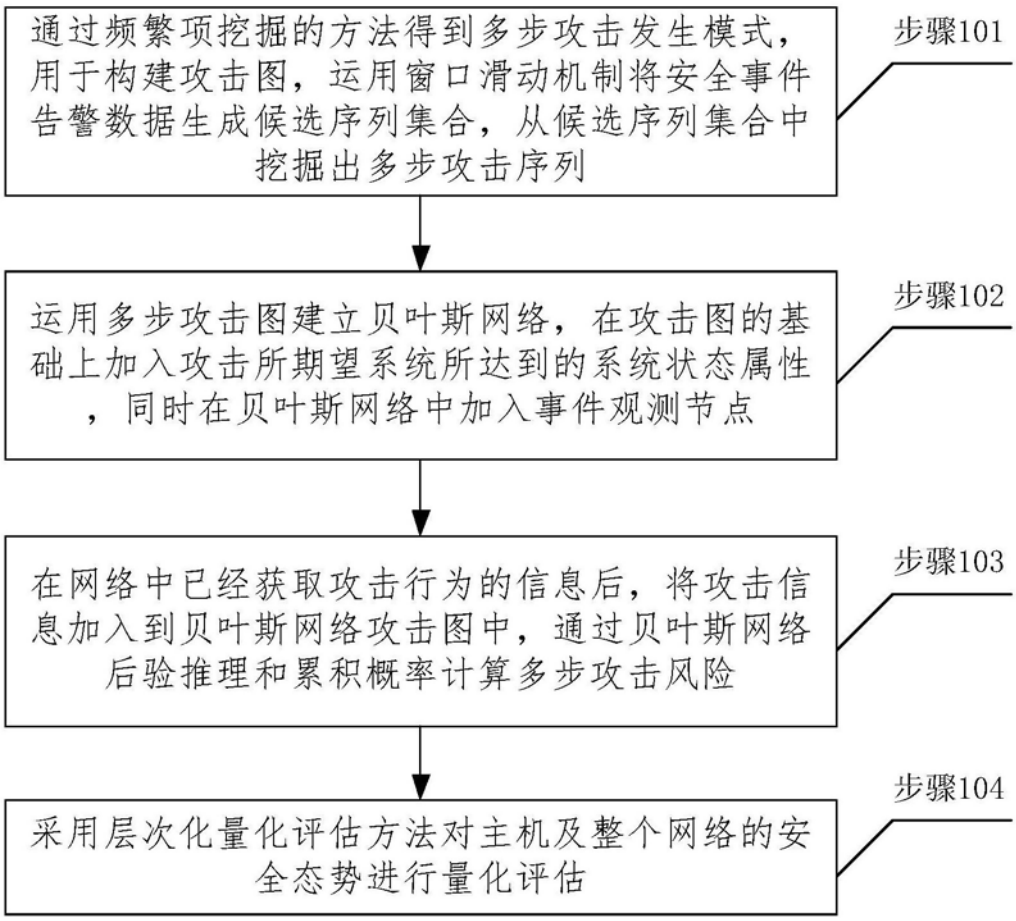

通过频繁项挖掘的方法得到多步攻击发生模式，用于构建攻击图，运用窗口滑动机制将安全事件告警数据生成候选序列集合，从候选序列集合中挖掘出多步攻击序列
步骤101
运用多步攻击图建立贝叶斯网络，在攻击图的基础上加入攻击所期望系统所达到的系统状态属性，同时在贝叶斯网络中加入事件观测节点
步骤102
在网络中已经获取攻击行为的信息后，将攻击信息加入到贝叶斯网络攻击图中，通过贝叶斯网络后验推理和累积概率计算多步攻击风险
步骤103
采用层次化量化评估方法对主机及整个网络的安全态势进行量化评估
步骤104

图1

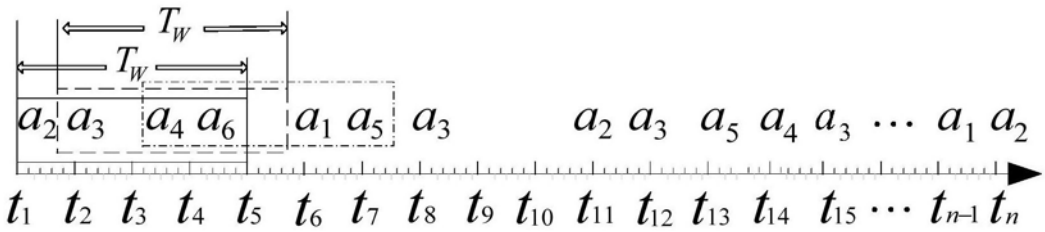

T_W
T_W
a_2 a_3 a_4 a_6 a_1 a_5 a_3 a_2 a_3 a_5 a_4 a_3 … a_1 a_2
t_1 t_2 t_3 t_4 t_5 t_6 t_7 t_8 t_9 t_{10} t_{11} t_{12} t_{13} t_{14} t_{15} … t_{n-1} t_n

图2

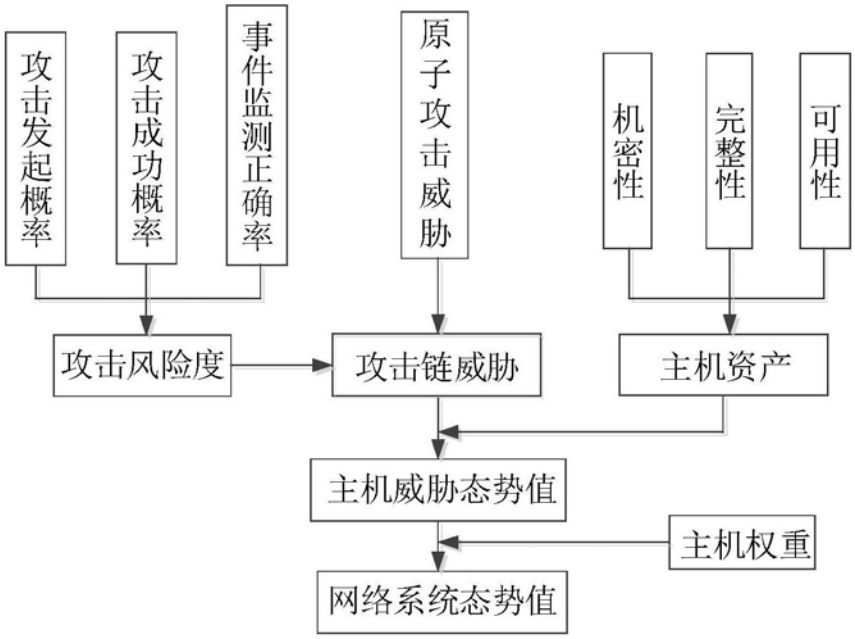

攻击发起概率
攻击成功概率
事件监测正确率
原子攻击威胁
机密性
完整性
可用性
攻击风险度
攻击链威胁
主机资产
主机威胁态势值
主机权重
网络系统态势值

图3

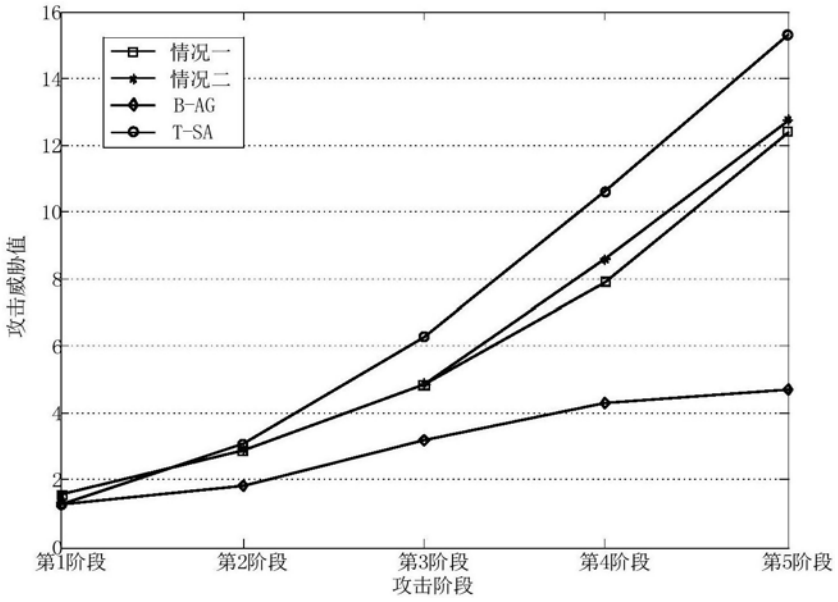

情况一
情况二
B-AG
T-SA
攻击威胁值
0
2
4
6
8
10
12
14
16
第1阶段
第2阶段
第3阶段
第4阶段
第5阶段
攻击阶段

图4

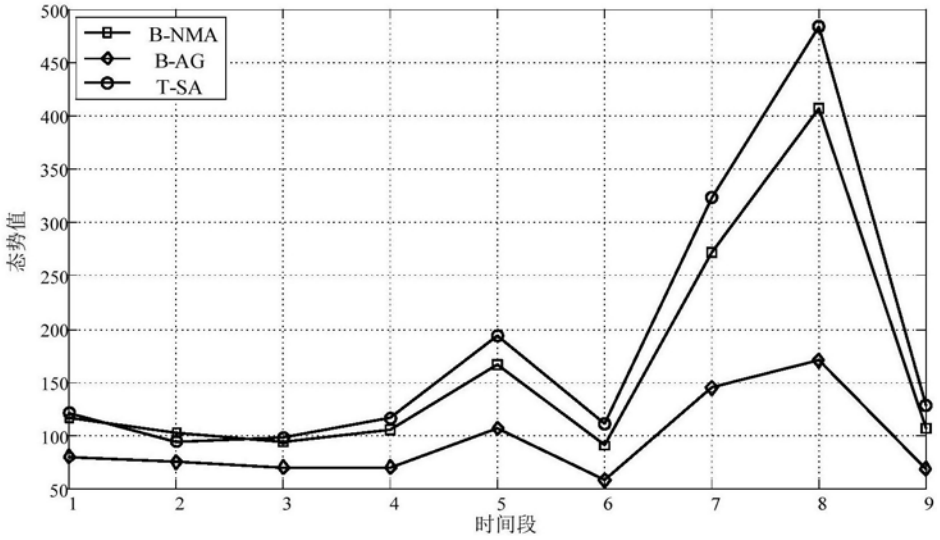

B-NMA
B-AG
T-SA
态势值
时间段
500
450
400
350
300
250
200
150
100
50
1
2
3
4
5
6
7
8
9

图5