(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117675413 A
(43)申请公布日 2024.03.08

(21)申请号 202410129795.X

(22)申请日 2024.01.31

(71)申请人 北京中关村实验室
地址 100089 北京市海淀区中关村东路1号院8号楼
申请人 北京航空航天大学

(72)发明人 高庆 王建峰 吕金虎 王薇 牛建伟 谭少林 郭一歌

(74)专利代理机构 北京超凡宏宇知识产权代理有限公司 11463
专利代理师 张波

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/10(2022.01)

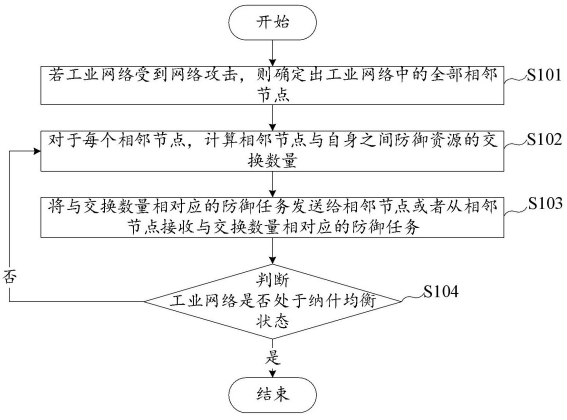
权利要求书3页 说明书18页 附图6页

(54)发明名称

受攻击工业节点间的防御资源分布式调度方法及装置

(57)摘要

本申请提供一种受攻击工业节点间的防御资源分布式调度方法及装置,涉及网络安全领域。其中,对于任意一个节点,若工业网络受到网络攻击,则确定出工业网络中的全部相邻节点,其中,每个相邻节点表示与自身相邻的节点;对于每个相邻节点,计算相邻节点与自身之间防御资源的交换数量;将与交换数量相对应的防御任务发送给相邻节点或者从相邻节点接收与交换数量相对应的防御任务;若与全部相邻节点进行资源交换后,工业网络未处于纳什均衡状态,则返回至对于每个相邻节点,计算相邻节点与自身之间防御资源的交换数量,直至工业网络处于纳什均衡状态。如此,由于防御资源仅在相邻节点之间进行调度,因此,能够极大提高资源调度效率。



CN 117675413 A

1.一种受攻击工业节点间的防御资源分布式调度方法,其特征在于,应用于工业网络中的任意一个节点,所述方法包括:

若所述工业网络受到网络攻击,则确定出所述工业网络中的全部相邻节点,其中,每个所述相邻节点表示与自身相邻的节点;

对于每个所述相邻节点,计算所述相邻节点与自身之间防御资源的交换数量;

将与所述交换数量相对应的防御任务发送给所述相邻节点或者从所述相邻节点接收与所述交换数量相对应的防御任务;

若与所述全部相邻节点进行资源交换后,所述工业网络未处于纳什均衡状态,则返回至对于每个所述相邻节点,计算所述相邻节点与自身之间防御资源的交换数量,直至所述工业网络处于纳什均衡状态。

2.根据权利要求1所述的受攻击工业节点间的防御资源分布式调度方法,其特征在于,所述对于每个所述相邻节点,计算所述相邻节点与自身之间防御资源的交换数量,包括:

获取自身防御资源以及受到的攻击资源、所述相邻节点的防御资源以及受到的攻击资源;

根据所述自身防御资源以及受到的攻击资源、所述相邻节点的防御资源以及受到的攻击资源,得到所述相邻节点与自身之间防御资源的交换数量。

3.根据权利要求2所述的受攻击工业节点间的防御资源分布式调度方法,其特征在于,所述根据所述自身防御资源以及受到的攻击资源、所述相邻节点的防御资源以及受到的攻击资源,得到所述相邻节点与自身之间防御资源的交换数量,包括:

根据所述自身的防御资源以及受到的攻击资源,得到自身被攻击成功的第一概率;

根据所述相邻节点的防御资源以及受到的攻击资源,得到所述相邻节点被攻击成功的第二概率;

根据自身的防御资源、所述相邻节点的防御资源、所述第一概率以及所述第二概率,计算得到所述相邻节点与自身之间防御资源的交换数量。

4.根据权利要求3所述的受攻击工业节点间的防御资源分布式调度方法,其特征在于,所述根据自身的防御资源、所述相邻节点的防御资源、所述第一概率以及所述第二概率,计算得到所述相邻节点与自身之间防御资源的交换数量,表达式为:

$$\Delta = x_d^j[F_i - F_j]_+ - x_d^i\left[F_j - F_i\right]_+;$$

式中,Δ表示所述交换数量,x_d^j表示第j个相邻节点的防御资源,x_d^i表示第i个节点的防御资源,$F_i(x_d)$表示第i个节点自身被攻击成功的第一概率,$F_j(x_d)$表示第j个相邻节点自身被攻击成功的第二概率;若$F_i - F_j > 0$,$[F_i - F_j]_+ = F_i - F_j$,$F_i - F_j \le 0$,$[F_i - F_j]_+ = 0$。

5.根据权利要求3所述的受攻击工业节点间的防御资源分布式调度方法,其特征在于,所述自身的防御资源包括直接参与网络防御的第一直接资源,所述根据所述自身的防御资源以及受到的攻击资源,得到自身被攻击成功的第一概率,表达式为:

$$F_i=\frac{x_a^i}{x_d^i+x_a^i+c};$$

式中，F_i表示工业网络中的第i个节点自身被攻击成功的第一概率，x_a^i表示第i个节点受到的攻击资源，x_d^i表示第i个节点自身的第一直接资源，c为大于0的常数。

6.根据权利要求3所述的受攻击工业节点间的防御资源分布式调度方法，其特征在于，所述相邻节点的防御资源包括直接参与网络防御的第二直接资源，根据所述相邻节点的防御资源以及受到的攻击资源，得到所述相邻节点被攻击成功的第二概率，表达式为：

$$F_j=\frac{x_a^j}{x_d^j+x_a^j+c};$$

式中，F_j表示第j个相邻节点自身被攻击成功的第二概率，x_a^j表示第j个相邻节点受到的攻击资源，x_d^j表示第j个相邻节点自身的第二直接资源，c为大于0的常数。

7.根据权利要求3所述的受攻击工业节点间的防御资源分布式调度方法，其特征在于，所述自身防御资源包括直接参与网络防御的第一直接资源以及间接支持网络防御的第一间接资源，所述根据所述自身的防御资源以及受到的攻击资源，得到自身被攻击成功的第一概率，表达式为：

$$F_i=\frac{x_a^i}{x_d^i+x_a^i+c}-r_i;$$

$$r_i=-Px_d^i+C_i;$$

式中，F_i表示第i个节点自身被攻击成功的第一概率，x_a^i表示第i个节点受到的攻击资源，x_d^i表示第i个节点自身的第一直接资源，r_i表示所述第一间接资源，c为常数，P表示预设比例系数，C_i表示与第i个节点初始防御资源相关的常数。

8.根据权利要求3所述的受攻击工业节点间的防御资源分布式调度方法，其特征在于，所述相邻节点的防御资源包括直接参与网络防御的第二直接资源以及间接支持网络防御的第二间接资源；根据所述相邻节点的防御资源以及受到的攻击资源，得到所述相邻节点被攻击成功的第二概率，表达式为：

$$F_j=\frac{x_a^j}{x_d^j+x_a^j+c}-r_j;$$

$$r_j=-Px_d^j+C_j;$$

式中，F_j表示第j个节点自身被攻击成功的第二概率，x_a^j表示第j个节点受到的攻击资源，x_d^j表示第j个节点自身的第二直接资源，r_j表示所述第二间接资源，c为大于0的常

数，P表示预设比例系数，C_j表示与j个节点初始防御资源相关的常数。

9.根据权利要求1所述的受攻击工业节点间的防御资源分布式调度方法，其特征在于，所述确定出所述工业网络中的全部相邻节点，包括：

获取预先为所述工业网络中的节点构建的无向连通图；

根据所述无向连通图，确定出所述工业网络中的全部相邻节点。

10.一种受攻击工业节点间的防御资源分布式调度装置，其特征在于，应用于工业网络中的任意一个节点，所述装置包括：

相邻节点模块，用于若所述工业网络受到网络攻击，则确定出所述工业网络中的全部相邻节点，其中，每个所述相邻节点表示与自身相邻的节点；

资源交互模块，用于对于每个所述相邻节点，计算所述相邻节点与自身之间防御资源的交换数量；

所述资源交互模块，还用于将与所述交换数量相对应的防御任务发送给所述相邻节点或者从所述相邻节点接收与所述交换数量相对应的防御任务；

资源迭代模块，用于若与所述全部相邻节点进行资源交换后，所述工业网络未处于纳什均衡状态，则返回至对于每个所述相邻节点，计算所述相邻节点与自身之间防御资源的交换数量，直至所述工业网络处于纳什均衡状态。

受攻击工业节点间的防御资源分布式调度方法及装置

技术领域

[0001] 本申请涉及网络安全领域,具体而言,涉及一种受攻击工业节点间的防御资源分布式调度方法及装置。

背景技术

[0002] 如图1所示,现阶段关于防御资源调度的研究有通常是通过一个集中式的资源调度中心在一个扁平化(全连通图结构)的节点网络上分配资源。

[0003] 图中,x_a^i表示攻击者的攻击资源,反映了攻击者的攻击强度;x_d^i表示集中式资源调度中心为工业网络100中的第i个节点上分配的防御资源,反映了节点的防御能力,$i=1,2,\cdots,n$,并满足:

$$\sum_{i=1}^{n} x_a^i \le X_a, \sum_{i=1}^{n} x_d^i \le X_d ;$$

式中,X_a表示攻击资源的整体预算,X_d表示防御资源的整体预算。此外,假定将攻击者给定攻击策略表示为:

$$x_a = (x_a^1, x_a^2, \cdots, x_a^n) \in \Delta_a \subseteq \mathrm{i}^{\,n};$$

则集中式的资源调度中心进行防御资源调度的最终的目标函数标识为:

$$F(x_d) = D(x_d) + C(x_d)$$

$$x_d = \left(x_d^1, x_d^2, \cdots, x_d^n\right) \in \Delta_d \subseteq \mathrm{i}^{\,n};$$

式中,$D(x_d)$表示工业网络100节点整体的受攻击损失,$C(x_d)$表示防御资源花费的花费。如此,构建出优化问题,求解最优的资源分配策略,即:

$$\min_{x_d} F(x_d)$$

$$s.t. \sum_{i=1}^{n} x_d^i \le X_d ;$$

然而,实践过程中发现,在工业网络100中引入集中式的资源调度中心,一方面增加了生产成本,需要为资源调度中心单独设站,同时增大了节点间资源传输和通讯的成本,使得防御效率不足;另一方面采用集中式的资源调度中心,会导致工业网络100更容易受到网络攻击的影响,如果攻击者能够破坏资源调度中心,则可以访问系统中的所有资源。这使得攻击者更容易使用单个攻击来破坏整个系统。

发明内容

[0004] 为了克服现有技术中的至少一个不足,本申请提供一种受攻击工业节点间的防御资源分布式及装置,具体包括:

第一方面,本申请提供一种受攻击工业节点间的防御资源分布式调度方法,应用于工业网络中的任意一个节点,所述方法包括:

若所述工业网络受到网络攻击,则确定出所述工业网络中的全部相邻节点,其中,每个所述相邻节点表示与自身相邻的节点;

对于每个所述相邻节点,计算所述相邻节点与自身之间防御资源的交换数量;

将与所述交换数量相对应的防御任务发送给所述相邻节点或者从所述相邻节点接收与所述交换数量相对应的防御任务;

若与所述全部相邻节点进行资源交换后,所述工业网络未处于纳什均衡状态,则返回至对于每个所述相邻节点,计算所述相邻节点与自身之间防御资源的交换数量,直至所述工业网络处于纳什均衡状态。

[0005] 结合第一方面的可选实施方式,所述对于每个所述相邻节点,计算所述相邻节点与自身之间防御资源的交换数量,包括:

获取自身防御资源以及受到的攻击资源、所述相邻节点的防御资源以及受到的攻击资源;

根据所述自身防御资源以及受到的攻击资源、所述相邻节点的防御资源以及受到的攻击资源,得到所述相邻节点与自身之间防御资源的交换数量。

[0006] 结合第一方面的可选实施方式,所述根据所述自身防御资源以及受到的攻击资源、所述相邻节点的防御资源以及受到的攻击资源,得到所述相邻节点与自身之间防御资源的交换数量,包括:

根据所述自身的防御资源以及受到的攻击资源,得到自身被攻击成功的第一概率;

根据所述相邻节点的防御资源以及受到的攻击资源,得到所述相邻节点被攻击成功的第二概率;

根据自身的防御资源、所述相邻节点的防御资源、所述第一概率以及所述第二概率,计算得到所述相邻节点与自身之间防御资源的交换数量。

[0007] 结合第一方面的可选实施方式,所述根据自身的防御资源、所述相邻节点的防御资源、所述第一概率以及所述第二概率,计算得到所述相邻节点与自身之间防御资源的交换数量,表达式为:

$$\Delta = x_d^j[F_i - F_j]_+ - x_d^i\left[F_j - F_i\right]_+;$$

式中,Δ表示所述交换数量,x_d^j表示第j个相邻节点的防御资源,x_d^i表示第i个节点的防御资源,$F_i(x_d)$表示第i个节点自身被攻击成功的第一概率,$F_j(x_d)$表示第j个相邻节点自身被攻击成功的第二概率;若$F_i - F_j > 0$,$[F_i - F_j]_+ = F_i - F_j$,$F_i - F_j \le 0$,$[F_i - F_j]_+ = 0$。

[0008] 结合第一方面的可选实施方式,所述自身的防御资源包括直接参与网络防御的第一直接资源,所述根据所述自身的防御资源以及受到的攻击资源,得到自身被攻击成功的第一概率,表达式为:

$$F_i=\frac{x_a^i}{x_d^i+x_a^i+c};$$

式中，F_i表示工业网络中的第i个节点自身被攻击成功的第一概率，x_a^i表示第i个节点受到的攻击资源，x_d^i表示第i个节点自身的第一直接资源，c为大于0的常数。

[0009] 结合第一方面的可选实施方式，所述相邻节点的防御资源包括直接参与网络防御的第二直接资源，所述根据相邻节点的防御资源以及受到的攻击资源，得到所述相邻节点被攻击成功的第二概率，表达式为：

$$F_j=\frac{x_a^j}{x_d^j+x_a^j+c};$$

式中，F_j表示第j个相邻节点自身被攻击成功的第二概率，x_a^j表示第j个相邻节点受到的攻击资源，x_d^j表示第j个相邻节点自身的第二直接资源，c为大于0的常数。

[0010] 结合第一方面的可选实施方式，所述自身防御资源包括直接参与网络防御的第一直接资源以及间接支持网络防御的第一间接资源，所述根据所述自身的防御资源以及受到的攻击资源，得到自身被攻击成功的第一概率，表达式为：

$$F_i=\frac{x_a^i}{x_d^i+x_a^i+c}-r_i;$$

$$r_i=-Px_d^i+C_i;$$

式中，F_i表示第i个节点自身被攻击成功的第一概率，x_a^i表示第i个节点受到的攻击资源，x_d^i表示第i个节点自身的第一直接资源，r_i表示所述第一间接资源，c为常数，P表示预设比例系数，C_i表示与第i个节点初始防御资源相关的常数。

[0011] 结合第一方面的可选实施方式，所述相邻节点的防御资源包括直接参与网络防御的第二直接资源以及间接支持网络防御的第二间接资源；所述根据相邻节点的防御资源以及受到的攻击资源，得到所述相邻节点自身被攻击成功的第二概率，表达式为：

$$F_j=\frac{x_a^j}{x_d^j+x_a^j+c}-r_j;$$

$$r_j=-Px_d^j+C_j;$$

式中，F_j表示第j个节点自身被攻击成功的第二概率，x_a^j表示第j个节点受到的攻击资源，x_d^j表示第j个节点自身的第二直接资源，r_j表示所述第二间接资源，c为大于0的常数，P表示预设比例系数，C_j表示与j个节点初始防御资源相关的常数。

[0012] 结合第一方面的可选实施方式，所述确定出所述工业网络中的全部相邻节点，包

括：

获取预先为所述工业网络中的节点构建的无向连通图；

根据所述无向连通图，确定出所述工业网络中的全部相邻节点。

[0013] 第二方面，本申请还提供一种受攻击工业节点间的防御资源分布式调度装置，应用于工业网络中的任意一个节点，所述装置包括：

相邻节点模块，用于若所述工业网络受到网络攻击，则确定出所述工业网络中的全部相邻节点，其中，每个所述相邻节点表示与自身相邻的节点；

资源交互模块，用于对于每个所述相邻节点，计算所述相邻节点与自身之间防御资源的交换数量；

所述资源交互模块，还用于将与所述交换数量相对应的防御任务发送给所述相邻节点或者从所述相邻节点接收与所述交换数量相对应的防御任务；

资源迭代模块，用于若与所述全部相邻节点进行资源交换后，所述工业网络未处于纳什均衡状态，则返回至对于每个所述相邻节点，计算所述相邻节点与自身之间防御资源的交换数量，直至所述工业网络处于纳什均衡状态。

[0014] 结合第二方面的可选实施方式，所述对于每个所述相邻节点，所述资源交互模块还具体用于：

获取自身防御资源以及受到的攻击资源、所述相邻节点的防御资源以及受到的攻击资源；

根据所述自身防御资源以及受到的攻击资源、所述相邻节点的防御资源以及受到的攻击资源，得到所述相邻节点与自身之间防御资源的交换数量。

[0015] 结合第二方面的可选实施方式，所述资源交互模块还具体用于：

根据所述自身的防御资源以及受到的攻击资源，得到自身被攻击成功的第一概率；

根据所述相邻节点的防御资源以及受到的攻击资源，得到所述相邻节点被攻击成功的第二概率；

根据自身的防御资源、所述相邻节点的防御资源、所述第一概率以及所述第二概率，计算得到所述相邻节点与自身之间防御资源的交换数量。

[0016] 结合第二方面的可选实施方式，所述根据自身的防御资源、所述相邻节点的防御资源、所述第一概率以及所述第二概率，计算得到所述相邻节点与自身之间防御资源的交换数量，表达式为：

$$\Delta = x_d^j[F_i - F_j]_+ - x_d^i\left[F_j - F_i\right]_+;$$

式中，Δ表示所述交换数量，x_d^j表示第j个相邻节点的防御资源，x_d^i表示第i个节点的防御资源，$F_i(x_d)$表示第i个节点自身被攻击成功的第一概率，$F_j(x_d)$表示第j个相邻节点自身被攻击成功的第二概率；若$F_i - F_j > 0$，$[F_i - F_j]_+ = F_i - F_j$，$F_i - F_j \le 0$，$[F_i - F_j]_+ = 0$。

[0017] 结合第二方面的可选实施方式，所述自身的防御资源包括直接参与网络防御的第

一直接资源,所述资源交互模块还具体用于:

$$F_i=\frac{x_a^i}{x_d^i+x_a^i+c};$$

式中,F_i表示工业网络中的第i个节点自身被攻击成功的第一概率,x_a^i表示第i个节点受到的攻击资源,x_d^i表示第i个节点自身的第一直接资源,c为大于0的常数。

[0018] 结合第二方面的可选实施方式,所述相邻节点的防御资源包括直接参与网络防御的第二直接资源,所述根据相邻节点的防御资源以及受到的攻击资源,得到所述相邻节点被攻击成功的第二概率,表达式为:

$$F_j=\frac{x_a^j}{x_d^j+x_a^j+c};$$

式中,F_j表示第j个相邻节点自身被攻击成功的第二概率,x_a^j表示第j个相邻节点受到的攻击资源,x_d^j表示第j个相邻节点自身的第二直接资源,c为大于0的常数。

[0019] 结合第二方面的可选实施方式,所述自身防御资源包括直接参与网络防御的第一直接资源以及间接支持网络防御的第一间接资源,所述根据所述自身的防御资源以及受到的攻击资源,得到自身被攻击成功的第一概率,表达式为:

$$F_i=\frac{x_a^i}{x_d^i+x_a^i+c}-r_i;$$

$$r_i=-Px_d^i+C_i;$$

式中,F_i表示第i个节点自身被攻击成功的第一概率,x_a^i表示第i个节点受到的攻击资源,x_d^i表示第i个节点自身的第一直接资源,r_i表示所述第一间接资源,c为常数,P表示预设比例系数,C_i表示与第i个节点初始防御资源相关的常数。

[0020] 结合第二方面的可选实施方式,所述相邻节点的防御资源包括直接参与网络防御的第二直接资源以及间接支持网络防御的第二间接资源;所述根据相邻节点的防御资源以及受到的攻击资源,得到所述相邻节点自身被攻击成功的第二概率,表达式为:

$$F_j=\frac{x_a^j}{x_d^j+x_a^j+c}-r_j;$$

$$r_j=-Px_d^j+C_j;$$

式中,F_j表示第j个节点自身被攻击成功的第二概率,x_a^j表示第j个节点受到的攻击资源,x_d^j表示第j个节点自身的第二直接资源,r_j表示所述第二间接资源,c为大于0的常数,P表示预设比例系数,C_j表示与j个节点初始防御资源相关的常数。

[0021] 结合第二方面的可选实施方式,所述相邻节点模块还具体用于:

获取预先为所述工业网络中的节点构建的无向连通图;

根据所述无向连通图,确定出所述工业网络中的全部相邻节点。

[0022] 相对于现有技术而言,本申请具有以下有益效果:

本申请提供一种受攻击工业节点间的防御资源分布式调度方法及装置,应用于工业网络中的任意一个节点。其中,若工业网络受到网络攻击,则确定出工业网络中的全部相邻节点,其中,每个相邻节点表示与自身相邻的节点;对于每个相邻节点,计算相邻节点与自身之间防御资源的交换数量;将与交换数量相对应的防御任务发送给相邻节点或者从相邻节点接收与交换数量相对应的防御任务;若与全部相邻节点进行资源交换后,工业网络未处于纳什均衡状态,则返回至对于每个相邻节点,计算相邻节点与自身之间防御资源的交换数量,直至工业网络处于纳什均衡状态。如此,由于防御资源仅在相邻节点之间进行调度,因此,能够极大提高资源调度效率。

附图说明

[0023] 为了更清楚地说明本申请实施例的技术方案,下面将对实施例中所需要使用的附图作简单地介绍,应当理解,以下附图仅示出了本申请的某些实施例,因此不应被看作是对范围的限定,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他相关的附图。

[0024] 图1为本申请实施例提供的现有资源调度原理示意图;

图2为本申请实施例提供的方法流程示意图;

图3为本申请实施例提供的相邻节点查找原理示意图;

图4为本申请实施例提供的无间接防御资源时的调度原理示意图;

图5为本申请实施例提供的有间接防御资源时的调度原理示意图;

图6为本申请实施例提供的验证网络的结构示意图;

图7为本申请实施例提供的验证效果示意图之一;

图8为本申请实施例提供的验证效果示意图之二;

图9为本申请实施例提供的虚拟装置的结构示意图;

图10为本申请实施例提供的电子设备的结构示意图。

[0025] 图标:100-工业网络;201-相邻节点模块;202-资源交互模块;203-资源迭代模块;301-存储器;302-处理器;303-通信单元;304-系统总线。

具体实施方式

[0026] 为使本申请实施例的目的、技术方案和优点更加清楚,下面将结合本申请实施例中的附图,对本申请实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例是本申请一部分实施例,而不是全部的实施例。通常在此处附图中描述和示出的本申请实施例的组件可以以各种不同的配置来布置和设计。

[0027] 因此,以下对在附图中提供的本申请的实施例的详细描述并非旨在限制要求保护的本申请的范围,而是仅仅表示本申请的选定实施例。基于本申请中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本申请保护的范

围。

[0028] 应注意到:相似的标号和字母在下面的附图中表示类似项,因此,一旦某一项在一个附图中被定义,则在随后的附图中不需要对其进行进一步定义和解释。

[0029] 在本申请的描述中,需要说明的是,术语“第一”、“第二”、“第三”等仅用于区分描述,而不能理解为指示或暗示相对重要性。

[0030] 此外,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0031] 基于以上声明,正如背景技术中所介绍的,目前集中式网络防御方式存在防御效率低、资源调度中心受攻击威胁等情况。具体表现为,现有资源调度技术的决策者为集中式的资源调度中心,也就是说资源调度中心依据每个节点受到的攻击资源,将防御资源都是从资源调度中心出发,分配到各个受攻击的节点上,这种分配方式使防御资源的利用效率降低。此外,现有集中式的资源调度方法为静态最优,在动态攻击下动态调度资源的效率很低。因为防御资源是从资源调度中心分配到各个节点上,那么为适应动态攻击,就需要将防御资源过剩的节点上的防御资源先传输回资源调度中心,再由资源调度中心分配到各个节点。上述资源调度方式依赖于与集中式的资源调度中心之间的交互,因而存在资源调度效率不足的问题。

[0032] 其中,能够反应网络攻击强度的攻击信息包括节点受到的攻击流量、攻击来源、漏洞利用、威胁情报、攻击频率、异常行为等。

[0033] 攻击流量,节点接收到来自攻击者发送的攻击流量,攻击流量的增加意味着攻击者正在以更大的规模进行攻击,从而增加了攻击程度的严重性。

[0034] 攻击来源,可以根据攻击流量中的IP地址、地理位置和攻击者使用的工具来确定攻击来源。如果攻击源自多个地区并在不断增加,可能意味着当前受到的网络攻击强度较高。

[0035] 漏洞利用,监测已知漏洞被攻击者利用的情况,可以通过分析漏洞利用的频率、漏洞修复的速度以及受影响系统的数量来评估当前受到的网络攻击强度,如果漏洞利用频繁或修复速度较慢,可能表示当前受到的网络攻击强度较高。

[0036] 威胁情报,威胁情报可以包括新发现的攻击技术、恶意软件变种、攻击者的新策略等,如果威胁情报中存在新的高级攻击技术或攻击策略,可能表示当前受到的网络攻击强度较高。

[0037] 攻击频率,指的是在一定时间内发生的网络攻击的次数。它表示了攻击者对目标网络或系统进行攻击的频繁程度。攻击频率是一个关键指标,可以用来评估当前网络受到的攻击强度。

[0038] 异常行为,使用行为分析技术来检测异常的活动模式,例如大量无效登录尝试、异常的文件访问或系统配置更改,这些异常行为可能是攻击者的迹象,需要进行防御检测。

[0039] 本实施例中,考虑到上述攻击信息分别具有不同的量纲,因此,节点持续检测上述攻击信息,并将检测出的上述攻击信息进行量化以及无量纲转换,从而得到节点受到的攻

击资源。

[0040] 而反映节点防御能力的防御信息包括硬件防御能力以及软件防御能力,其中,硬件防御能力包括节点的CPU算力、内存容量、内存读写速度、磁盘容量、磁盘读写速度、网络带宽等;而软件防御能力则包括节点中部署的防御软件的数量。本实施例中,将上述防御信息同样进行量化以及无量纲转换,从而得到节点的防御能力。

[0041] 结合上述示例可以看出,本实施例中的防御资源实际是与节点自身硬件资源以及软件资源,而这些资源实际并不能在节点之间的传输,因此,上述实施例中的资源调度并非指对上述硬件防御资源与软件防御资源进行调度,而是指将防御任务在节点之间进行调度。可以理解为,当一个节点需要从其他节点获取防御资源,表示节点自身防御资源不足,需要将自身的防御任务发送给其他节点;而一个节点需向其他节点提供防御资源,则表示自身防御资源过剩,可以帮其他节点进行防御任务的计算。上述防御任务则指提供识别正常访问与异常访问、漏洞管理与修复、安全监控和日志分析、访问权限管理等功能的人物。并且,防御任务对防御资源的消耗满足预设映射关系,因此,可以将需要调度的防御资源换算为能够消耗这些防御资源的防御任务的数量。

[0042] 基于上述技术问题的发现,发明人经过创造性劳动提出下述技术方案以解决或者改善上述问题。需要注意的是,以上现有技术中的方案所存在的缺陷,是发明人在经过实践并仔细研究后得出的结果,因此,上述问题的发现过程以及下文中本申请实施例针对上述问题所提出的解决方案,都应该是发明人在发明创造过程中对本申请做出的贡献,而不应当理解为本领域技术人员所公知的技术内容。

[0043] 研究发现,目前集中式的资源调度方式之所以资源调度效率不足,是因为集中式的资源调度方案是从系统整体利益最大的角度做出决策,没有考虑到当前工业网络环境下中每个节点都可以作为决策的主体,拥有一定的计算以及存储能力。鉴于此,本实施例提供一种受攻击工业节点间的防御资源分布式调度方法,应用于工业网络中的任意一个节点,用于使得每个节点不再依赖于资源调度中心,而是独立进行资源调度,使得整个工业网络中的节点趋近于平衡。该方法中,若工业网络受到网络攻击,则确定出工业网络中的全部相邻节点,其中,每个相邻节点表示与自身相邻的节点;对于每个相邻节点,计算相邻节点与自身之间防御资源的交换数量;将与交换数量相对应的防御任务发送给相邻节点或者从相邻节点接收与交换数量相对应的防御任务;若与全部相邻节点进行资源交换后,工业网络未处于纳什均衡状态,则返回至对于每个相邻节点,计算相邻节点与自身之间防御资源的交换数量,直至工业网络处于纳什均衡状态。如此,由于在遇到网络攻击后,防御资源仅在相邻节点之间进行调度,因此,能够极大提高资源调度效率。

[0044] 并且,由于不再具有资源调度中心,因此,能够避免资源调度中心被攻击后,整个网络被随意访问。

[0045] 本实施例中,上述工业网络中的所有节点可以是同一类型的设备,还可以是不同类型的设备。例如,这些节点可以是,但不限于,防火墙设备、代理服务器、虚拟专用网络设备、网关、路由器、交换机等。这些设备之间直接或者间接通信连接,使得彼此之间能够进行防御资源的调度。

[0046] 为使本实施例提供的方案更加清楚,下面结合图2对该方法的各个步骤进行详细阐述。但应该理解,流程图的操作可以不按顺序实现,没有逻辑的上下文关系的步骤可以反

转顺序或者同时实施。此外,本领域技术人员在本申请内容的指引下,可以向流程图添加一个或多个其他操作,也可以从流程图中移除一个或多个操作。如图2所示,该方法包括:

S101,若工业网络受到网络攻击,则确定出工业网络中的全部相邻节点。

[0047] 其中,每个相邻节点表示与自身相邻的节点。此处应理解的是,工业网络受到网络攻击并不意味着每个节点受到了攻击,但任意一个节点受到网络攻击后,需要整个工业网络中的所有节点联动起来进行网络防御。本实施例中,为工业网络中的全部建立预先构建有无向连通图,因此,对于每个节点,获取预先为工业网络中的节点构建的无向连通图;根据无向连通图,确定出工业网络中的全部相邻节点。

[0048] 在无相连通图中,图中的边没有方向性,即连接两个节点的边可以同时被看作是从一个节点到另一个节点的路径,也可以反过来看作是从另一个节点到一个节点的路径。这意味着在无向连通图中,从一个顶点出发,可以通过一系列的边到达图中的任意其他节点。由于本实施例去掉了资源调度中心,因此,通过无相连通图可以将防御资源在节点之间无障碍调度。

[0049] 示例性的,如图3所示,图中示出了包括n个节点的工业网络100,对于该工业网络100,攻击者可以同时对n个节点发起攻击,或者对其中一部分节点发起攻击。在图3所示的无相连通图中,节点2的相邻节点包括节点1、3,节点4的相邻节点为节点3。

[0050] 结合上述实施例对相邻节点的介绍,继续参见图2,本实施例提供的受攻击工业节点间的防御资源分布式调度方法还包括:

S102,对于每个相邻节点,计算相邻节点与自身之间防御资源的交换数量;

作为可选实施方式,节点自身与防御节点之间需要交换的防御资源不仅与节点自身防御资源以及受到的攻击资源,还与相邻节点的防御资源以及受到的攻击资源相关,因此,步骤S102可以包括:

S102-1,获取自身防御资源以及受到的攻击资源、相邻节点的防御资源以及受到的攻击资源。

[0051] S102-2,根据自身防御资源以及受到的攻击资源、相邻节点的防御资源以及受到的攻击资源,得到相邻节点与自身之间防御资源的交换数量。

[0052] 此处应理解的是,节点自身的防御资源与相邻节点的防御资源,均是两者当前可用的防御资源。研究还发现,对于节点或者该节点的相邻节点,自身防御资源以及受到的攻击资源之间的大小关系,直接影响被攻击成功的概率。例如,当防御资源远远小于攻击资源时,则会增加被攻击成功的概率,反之,则降低被攻击成功的概率。因此,步骤S102-2可以包括:

S102-21,根据自身的防御资源以及受到的攻击资源,得到自身被攻击成功的第一概率。

[0053] S102-22,根据相邻节点的防御资源以及受到的攻击资源,得到相邻节点被攻击成功的第二概率。

[0054] 作为步骤S102-21的可选实施方式,节点自身的防御资源包括直接参与网络防御的第一直接资源,例如,节点的处理器性能、内存大小、磁盘访问速度等。示例性的,如图4所示,继续用x_a^i表示第i个节点受到的攻击资源,x_d^i表示第i个节点在当前可用的直接防御

资源，$i=1,2,\cdots n$，并满足以下关系：

$$\sum_{i=1}^{n}x_a^i\le X_a,\sum_{i=1}^{n}x_d^i\le X_d;$$

式中，X_a表示攻击资源的整体预算，X_d表示防御资源的整体预算，记资源向量的可行域为Δ_d：

$$\Delta_d=\left\{x_d=(x_d^1,x_d^2,\cdots,x_d^n)^T\in \mathbb{i}^{\ n}:x_d^i\ge 0,\sum_{i=1}^{n}x_d^i=X_d\right\};$$

本实施例中工业网络100中节点交互的拓扑结构为无向连通图$\varsigma=\{V,\varepsilon\}$，其中，$V=\{1,2,\cdots,n\}$表示工业网络100中节点的集合，同时也可指代演化博弈中的策略集合；$\varepsilon\subseteq V\times V$表示是图中无向边的集合，因此，若$(i,j)\in\varepsilon$表示第$i$个节点与第$j$个节点相邻，两者之间可进行防御资源的传输。

[0055] 基于上述声明，根据自身的防御资源以及受到的攻击资源，得到自身被攻击成功的第一概率，表达式为：

$$F_i=\frac{x_a^i}{x_d^i+x_a^i+c};$$

式中，F_i表示工业网络100中的第i个节点自身被攻击成功的第一概率，x_a^i表示第i个节点受到的攻击资源，x_d^i表示第i个节点自身的第一直接资源，c为大于0的常数，用于确保x_a^i与x_d^i均为0时，该表达式仍然有效。

[0056] 同理，作为步骤S102-22的可选实施方式，相邻节点的防御资源包括直接参与网络防御的第二直接资源，根据相邻节点的防御资源以及受到的攻击资源，得到相邻节点被攻击成功的第二概率，表达式为：

$$F_j=\frac{x_a^j}{x_d^j+x_a^j+c};$$

式中，F_j表示第j个相邻节点自身被攻击成功的第二概率，x_a^j表示第j个相邻节点受到的攻击资源，x_d^j表示第j个相邻节点自身的第二直接资源，c为大于0的常数，用于确保x_a^j与x_d^j均为0时，该表达式仍然有效。

[0057] 此外，研究还发现，节点的防御能力，除了与直接参与防御的硬件资源以及软件资源相关，还与支撑节点进行防御的间接资源相关，例如，资金储备、网络复杂程度、能源支持、关键设备隐秘程度等。因此，在其他可选实施方式中，在计算被攻击成功的概率时，还引入了间接防御资源。并且，经过研究后发现，每个节点所具有的间接防御资源与该节点的直接防御资源满足特定比例关系，因此，本实施例还引入间接防御资源作为计算被攻击成功概率的惩罚因子，该惩罚因子实际反映了若节点要降低被成功攻击的概率外，则需要保持

其他间接资源的丰富性。

[0058] 示例性的，如图5所示，继续用x_a^i表示第i个节点受到的攻击资源，x_d^i表示第i个节点在当前可用的直接防御资源，$i=1,2,\cdots n$，并满足以下关系：

$$\sum_{i=1}^{n} x_a^i \le X_a, \sum_{i=1}^{n} x_d^i \le X_d;$$

式中，X_a表示攻击资源的整体预算，X_d表示防御资源的整体预算，记资源向量的可行域为Δ_d：

$$\Delta_d = \left\{ x_d = (x_d^1, x_d^2, \cdots, x_d^n)^T \in \mathrm{i}^{\ n} : x_d^i \ge 0, \sum_{i=1}^{n} x_d^i = X_d \right\};$$

而r_i为第i个节点在当前的间接资源(如资金、能源等)，满足$\sum_{i=1}^{n} r_i = R$；并且，本实施例中工业网络100中节点交互的拓扑结构为无向连通图$\varsigma = \{V, \varepsilon\}$，其中，$V = \{1,2,\cdots,n\}$表示工业网络100中节点的集合，同时也可指代演化博弈中的策略集合；$\varepsilon \subseteq V \times V$表示是图中无向边的集合，因此，若$(i,j) \in \varepsilon$表示第$i$个节点与第$j$个节点相邻，两者之间可进行防御资源的传输。

[0059] 基于上述声明，作为步骤S102-21的其他可选实施方式，节点自身防御资源包括直接参与网络防御的第一直接资源以及间接支持网络防御的第一间接资源，根据自身的防御资源以及受到的攻击资源，得到自身被攻击成功的第一概率，表达式为：

$$F_i = \frac{x_a^i}{x_d^i + x_a^i + c} - r_i;$$

$$r_i = -P x_d^i + C_i;$$

式中，F_i表示工业网络100中的第i个节点自身被攻击成功的第一概率，x_a^i表示第i个节点受到的攻击资源，x_d^i表示第i个节点自身的第一直接资源，r_i表示第一间接资源，c为大于0的常数，用于确保x_a^i与x_d^i均为0时，该表达式仍然有效，P表示预设比例系数，C_i表示与第i个节点初始防御资源相关的常数。

[0060] 作为步骤S102-22的其他可选实施方式，相邻节点的防御资源包括直接参与网络防御的第二直接资源以及间接支持网络防御的第二间接资源；根据相邻节点的防御资源以及受到的攻击资源，得到相邻节点自身被攻击成功的第二概率，表达式为：

$$F_j = \frac{x_a^j}{x_d^j + x_a^j + c} - r_j;$$

$$r_j = -P x_d^j + C_j;$$

式中，F_j表示第j个节点自身被攻击成功的第二概率，x_a^j表示第j个节点受到的攻击资源，x_d^j表示第j个节点自身的第二直接资源，r_j表示第二间接资源，c为大于0的常数，用于确保x_a^j与x_d^j均为0时，该表达式仍然有效，P表示预设比例系数，C_j表示与第j个节点初始防御资源相关的常数。

[0061] 结合上述实施例关于第一概率与第二概率的介绍，上述步骤S102-2还包括：

S102-23，根据自身的防御资源、相邻节点的防御资源、第一概率以及第二概率，计算得到相邻节点与自身之间防御资源的交换数量。

[0062] 作为可选实施方式，根据自身的防御资源、相邻节点的防御资源、第一概率以及第二概率，计算得到相邻节点与自身之间防御资源的交换数量，表达式为：

$$\Delta = x_d^j[F_i - F_j]_+ - x_d^i\left[F_j - F_i\right]_+;$$

式中，Δ表示交换数量，x_d^j表示第j个相邻节点的防御资源，x_d^i表示第i个节点的防御资源，$F_i(x_d)$表示第i个节点自身被攻击成功的第一概率，$F_j(x_d)$表示第j个相邻节点自身被攻击成功的第二概率；若$F_i - F_j > 0$，$[F_i - F_j]_+ = F_i - F_j$，$F_i - F_j \le 0$，$[F_i - F_j]_+ = 0$；同理，若$F_j - F_i > 0$，$[F_j - F_i]_+ = F_j - F_i$，$F_j - F_i \le 0$，$[F_j - F_i]_+ = 0$。

[0063] 以上实施例以工业网络100中的第i个节点为例，介绍了其与一个相邻节点之间如何确定御资源的交换数量。假定对于第i节点，其相邻节点的集合表示为N_i个，则第i节点在本次迭代过程中需要与集合N_i中相邻节点之间交换的防御资源之和表示为Δ_{sum}，其表达式为：

$$\Delta_{sum} = \sum_{j\in N_i} x_d^j[F_i(x_d) - F_j(x_d)]_+ - \sum_{j\in N} x_d^i[F_j(x_d) - F_i(x_d)]_+$$

[0064] 结合上述实施例对防御资源的交换数量介绍，继续参见图2，本实施例提供的受攻击工业节点间的防御资源分布式调度方法还包括：

S103，将与交换数量相对应的防御任务发送给相邻节点或者从相邻节点接收与交换数量相对应的防御任务。

[0065] 对此，正如上述中所介绍的，实施例中的资源调度并非指对节点上的硬件防御资源与软件防御资源进行调度，而是指将防御任务在节点之间进行调度。并且，防御任务对防御资源的消耗满足预设映射关系，因此，可以将需要调度的防御资源换算为能够消耗这些防御资源的防御任务的数量。

[0066] 如此，对于工业网络中的每个节点，在本次迭代过程中均与自身相邻节点之间进行防御资源交换，意味着本次迭代完成后，至少一部分节点剩余的防御资源会增加或者减少。继续参见图2，本实施例提供的受攻击工业节点间的防御资源分布式调度方法还包括：

S104，判断工业网络是否处于纳什均衡状态，若否，则返回步骤S102，若是，则结束

与相邻节点之间进行防御资源调度。

[0067] 本实施例中,对于工业网络中每个节点,其防御资源的梯度变化小于设定阈值时,视为工业网络处于纳什均衡状态。对此,应理解的到的是,当工业网络中的全部节点处于纳什均衡状态时,意味着在当前的情况下,没有任何一个节点可以通过单独改变其防御策略来获得更好的结果。换句话说,每个节点都选择了一种防御策略,给定其他节点的策略不变,它们没有任何激励来单独改变自己的策略。其中,纳什均衡是博弈论中的一个概念,用于描述多方参与的博弈中的稳定状态。在本实施例中,可以将每个节点看作是博弈中的参与者,它们通过选择不同的防御策略来应对潜在的攻击或威胁。当网络的防御状态处于纳什均衡时,意味着每个节点已经选择了最优的防御策略,考虑到其他节点的策略。在这种状态下,没有节点能够通过单方面改变策略来获得更大的收益或更好的防御效果。因此,纳什均衡表示一种稳定的防御状态,其中每个节点都采取了最佳的应对策略,并且没有动机单独改变它们的策略。

[0068] 而想要达到纳什均衡状态,则需要工业网络中存在纳什均衡,即需要具有均衡存在性与均衡唯一性。本实施将节点间防御资源的迁移过程视为演化博弈过程,并提出第i个节点的适应性函数F_i:

$$F_i=\frac{x_a^i}{x_d^i+x_a^i+c},c>0;$$

上述适应性函数,基于在不考虑间接防御资源的情况下,记:

$$f(x_d)=\sum_{i\in V}x_a^i ln(x_d^i+x_a^i+c);$$

式中,V表示节点的集合,i表示集合V中的第i个节点,x_a^i表示第i个节点受到的攻击资源,x_d^i表示第i个节点可用的防御资源,c表示常数。则基于上述表达式,证明过程如下:

均衡存在性:

上述表达式,满足$\frac{\partial f(x_d)}{\partial x_d^i}=F_i$,说明该演化博弈是全势博弈,将$F_i$视为演化博弈中第$i$个节点的适应性函数,表征第$i$个节点被成功攻击的概率。则对所有$x_d(0)\in\Delta_d$的节点初始防御资源的所有量,当迭代的时间$t\to\infty$时,都会到达广义的纳什均衡点。下面对此进行详细证明:

定义李雅普诺夫函数$V(x_d)=\overline{f}-f(x_d)$,其中,$\overline{f}=\max_{x_d\in\Delta_d}f(x_d)$,则显然$V(x_d)\geq 0$,则进一步可得以下表达式:

$$\dot{V}(x_d)=-\nabla f(x_d)^T\dot{x}_d=-F(x_d)^T\dot{x}_d;$$

式中,$F(x_d)=\left(F_i,F_2,\cdots F_n\right)^T$为集合$V$中$n$个工业节点的适应性函数组成的

向量，$F(x_d)^T\dot{x}_d$的表达式为：

$$F(x_d)^T\dot{x}_d=\sum_{i\in V}\sum_{j\in N_i}x_d^j\left[F_i-F_j\right]_+F_i-\sum_{i\in V}\sum_{j\in N_i}x_d^i\left[F_j-F_i\right]_+F_j$$
$$=\sum_{i\in V}\sum_{j\in N_i}x_d^j\left[F_i-F_j\right]_+F_i-\sum_{i\in V}\sum_{j\in N_i}x_d^i\left[F_j-F_i\right]_+F_j\quad;$$
$$=\sum_{i\in V}\sum_{j\in N_i}x_d^j\left[F_i-F_j\right]_+\left[F_i-F_j\right]$$

式中，明显可以看出$\left[F_i-F_j\right]_+\left[F_i-F_j\right]\geq 0$，意味着$F(x_d)^T\dot{x}_d\geq 0$，则可以得到：

$$\dot{V}(x_d)=-F(x_d)^T\dot{x}_d\leq 0;$$

因此，上述提出的用于节点防御资源更新的适应性函数是全局李雅普诺夫稳定的。

[0069] 均衡唯一性：

由于上述实施例提出的演化博弈是全势博弈，而以下表达式为凹函数：

$$f(x_d)=\sum_{i\in V}x_a^i ln(x_d^i+x_a^i+c);$$

因此，故纳什均衡问题存在唯一解。

[0070] 以上证明过程表明，工业网络中的节点按照上述适应性函数对节点防御资源存在纳什均衡状态，因此，只需要保证节点网络拓扑结构是连通图即可保证分布式资源调度算法在给定攻击者的攻击决策后，存在唯一的防御资源分布纳什均衡点。这就使得每个节点并不需要工业网络中其他全部节点的防御资源和适应性函数，只需要其相邻节点的防御资源量和适应性函数即可，因此，可以大大降低了通讯成本。同时，由于每个节点在本次迭代过程中防御资源的变化总量只和相邻节点的状态信息有关，使得节点间可以进行资源的直接传输，而不需要先传给资源调度中心，由资源调度中心分配给各个节点，进一步说明使用分布式动态调度的方法可以在攻击者的攻击决策发生变化时，系统响应时间较小，防御效率提高。

[0071] 同理，在引入间接防御资源后，首先不改变节点原有的适应性函数F_i，将间接防御资源与直接防御资源的交换率为定值，记为P。则工业网络中的第i个节点在本次迭代过程中间接防御资源的变化情况表示为∇_r：

$$\Delta_r=-\sum_{j\in N_i}x_d^jP\left[F_i-F_j\right]_++\sum_{j\in N_i}x_d^iP\left[F_j-F_i\right]_+=-P\Delta_{sum};$$

因此，即在适应性函数不变的情况下，并且间接防御资源与直接防御资源的交换率为定值时，间接资源的变化率Δ_r只与节点自身的直接防御资源变化率有关。进而在给定的$x_d(0)$和$r(0)$，有$r_i=-Px_d^i+C_i$，C_i表示与第i个节点初始防御资源相关常数。

[0072] 将上述间接防御资源作为惩罚项引入节点的适应性函数F_i，可得新的适应性函数$\tilde{F}_i$：

$$\tilde{F}_i=\frac{x_a^i}{x_d^i+x_a^i+c}-r_i=\frac{x_a^i}{x_d^i+x_a^i+c}+Px_d^i-C_i;$$

该新的适应性函数表明，若节点想要降低被成功攻击的概率外，还需要同时要保持间接防御资源的丰富性。并且，在引入间接防御资源后，节点的适应性函数本质上仍然只依赖于节点上的攻击资源和直接防御资源。并且，基于上述适应性函数，在考虑间接防御资源的情况下，记：

$$\tilde{f}(x_d,r)=\sum_{i\in V}x_a^i\ln(x_d^i+x_a^i)-\frac{1}{2P}r_i^2+\frac{C_i}{p}r_i-\frac{C_i^2}{2P};$$

可以得到，$\nabla_{x_d}\tilde{f}(x_d,r)=\tilde{F}_i$，即在考虑间接防御资源的情况下，工业网络中节点之间防御资源调度演化仍为全势博弈，存在博弈过程中的纳什均衡状态，且由于$\tilde{f}(x_d,r)$为关于x_d的凹函数，因而，同样存在均衡唯一性。

[0073] 对于上述实施例，本实施例还利用实际数据进行了验证。如图6所示，假定工业网络100中的节点的数量$n=10$，这10个节点之间的网络拓扑结构为无相连通图。对于这10个节点，为其提供初始的直接防御资源为$x_d(0)$：

$$x_d(0)=[0,0.2,0,0.3,0.1,0,0.1,0.1,0,0.2];$$

初始的间接防御资源为$r(0)$：

$$r(0)=[0,0,0,0,0,0,0,0,0,0];$$

并假定这10个节点受到的攻击资源位$x_a(0)$，直接防御资源与间接防御资源之间的比例系数$P=0.1$：

$$x_a(0)=[0,0.15,0,0.1,0.125,0.125,0.125,0.125,0.125,0.125]$$

[0074] 基于上述初始数据，如图7所示，由图中10个节点的防御资源随时间的变化曲线不难看出，各节点依据上述适应性函数与相邻节点进行分布式的资源调度，并最终达到纳什均衡状态，并且均衡存在且唯一。整个防御策略的动态调整过程，无需资源调度中心统一分配，而是根据相邻节点的状态信息生成的变化率自主传输。

[0075] 如图8所示，在$t=50$时，攻击者改变其攻击决策，使得10个节点受到的攻击资源变为：

$$x_a(50)=[0.15,0.1,0.125,0.125,0.05,0.125,0.2,0,0,0.125];$$

此时，工业网络100中的节点能够快速响应攻击资源的变化，重新调度防御资源在节点之间的分配，重新达到纳什均衡状态。

[0076] 基于与本实施例所提供一种受攻击工业节点间的防御资源分布式调度方法相同的发明构思,本实施例还提供一种受攻击工业节点间的防御资源分布装置,该装置包括至少一个可以软件形式存储于存储器或固化在电子设备中的软件功能模块。电子设备中的处理器用于执行存储器中存储的可执行模块。例如,受攻击工业节点间的防御资源分布式装置所包括的软件功能模块及计算机程序等。请参照图9,从功能上划分,受攻击工业节点间的防御资源分布式及装置可以包括:

相邻节点模块201,用于若工业网络受到网络攻击,则确定出工业网络中的全部相邻节点,其中,每个相邻节点表示与自身相邻的节点;

资源交互模块202,用于对于每个相邻节点,计算相邻节点与自身之间防御资源的交换数量;

资源交互模块202,还用于将与交换数量相对应的防御任务发送给相邻节点或者从相邻节点接收与交换数量相对应的防御任务;

资源迭代模块203,用于若与全部相邻节点进行资源交换后,工业网络未处于纳什均衡状态,则返回至对于每个相邻节点,计算相邻节点与自身之间防御资源的交换数量,直至工业网络处于纳什均衡状态。

[0077] 在本实施例中,上述相邻节点模块201用于实现图2中的步骤S101,资源交互模块202用于实现图2中的步骤S102、S103,资源迭代模块203用于实现图2中的步骤S104。关于上述各模块的详细描述可以参见对应步骤的具体实施方式,本实施例不再进行赘述。值得说明的是,由于与受攻击工业节点间的防御资源分布式调度方法具有相同的发明构思,因此,上述模块还可以用于实现该方法的其他步骤或者子步骤。

[0078] 另外,在本申请各个实施例中的各功能模块可以集成在一起形成一个独立的部分,也可以是各个模块单独存在,也可以两个或两个以上模块集成形成一个独立的部分。

[0079] 还应理解的是,以上实施方式如果以软件功能模块的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。基于这样的理解,本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本申请各个实施例所述方法的全部或部分步骤。

[0080] 因此,本实施例还提供一种存储介质,该存储介质存储有计算机程序,该计算机程序被处理器执行时,实现本实施例提供的受攻击工业节点间的防御资源分布式调度方法。其中,该存储介质可以是U盘、移动硬盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0081] 本实施例提供的一种用于实施上述受攻击工业节点间的防御资源分布式调度方法的电子设备。如图10所示,该电子设备可包括处理器302及存储器301。并且,存储器301存储有计算机程序,处理器通过读取并执行存储器301中与以上实施方式对应的计算机程序,实现本实施例所提供的受攻击工业节点间的防御资源分布式调度方法。

[0082] 继续参见图10,该电子设备还包括有通信单元303。该存储器301、处理器302以及通信单元303各元件相互之间通过系统总线304直接或间接地电性连接,以实现数据的传输或交互。

[0083] 其中,该存储器301可以是基于任何电子、磁性、光学或其它物理原理的信息记录装置,用于记录执行指令、数据等。在一些实施方式中,该存储器301可以是,但不限于,易失存储器、非易失性存储器、存储驱动器等。

[0084] 在一些实施方式中,该易失存储器可以是随机存取存储器(Random Access Memory,RAM);在一些实施方式中,该非易失性存储器可以是只读存储器(Read Only Memory,ROM)、可编程只读存储器(Programmable Read-Only Memory,PROM)、可擦除只读存储器(Erasable Programmable Read-Only Memory,EPROM)、电可擦除只读存储器(Electric Erasable Programmable Read-Only Memory,EEPROM)、闪存等;在一些实施方式中,该存储驱动器可以是磁盘驱动器、固态硬盘、任何类型的存储盘(如光盘、DVD等),或者类似的存储介质,或者它们的组合等。

[0085] 该通信单元303用于通过网络收发数据。在一些实施方式中,该网络可以包括有线网络、无线网络、光纤网络、远程通信网络、内联网、因特网、局域网(Local Area Network,LAN)、广域网(Wide Area Network,WAN)、无线局域网(Wireless Local Area Networks,WLAN)、城域网(Metropolitan Area Network,MAN)、广域网(Wide Area Network,WAN)、公共电话交换网(Public Switched Telephone Network,PSTN)、蓝牙网络、ZigBee网络、或近场通信(Near Field Communication,NFC)网络等,或其任意组合。在一些实施例中,网络可以包括一个或多个网络接入点。例如,网络可以包括有线或无线网络接入点,例如基站和/或网络交换节点,服务请求处理系统的一个或多个组件可以通过该接入点连接到网络以交换数据和/或信息。

[0086] 该处理器302可能是一种集成电路芯片,具有信号的处理能力,并且,该处理器可以包括一个或多个处理核(例如,单核处理器或多核处理器)。仅作为举例,上述处理器可以包括中央处理单元(Central Processing Unit,CPU)、专用集成电路(Application Specific Integrated Circuit,ASIC)、专用指令集处理器(Application Specific Instruction-set Processor,ASIP)、图形处理单元(Graphics Processing Unit,GPU)、物理处理单元(Physics Processing Unit,PPU)、数字信号处理器 (Digital Signal Processor,DSP)、现场可编程门阵列(Field Programmable Gate Array,FPGA)、可编程逻辑器件(Programmable Logic Device,PLD)、控制器、微控制器单元、简化指令集计算机(Reduced Instruction Set Computing,RISC)、或微处理器等,或其任意组合。

[0087] 可以理解,图10所示的结构仅为示意。电子设备还可以具有比图10所示更多或者更少的组件,或者具有与图10所示不同的配置。图10所示的各组件可以采用硬件、软件或其组合实现。

[0088] 应该理解到的是,在上述实施方式中所揭露的装置和方法,也可以通过其它的方式实现。以上所描述的装置实施例仅仅是示意性的,例如,附图中的流程图和框图显示了根据本申请的多个实施例的装置、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上,流程图或框图中的每个方框可以代表一个模块、程序段或代码的一部分,所述模块、程序段或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意,在有些作为替换的实现方式中,方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如,两个连续的方框实际上可以基本并行地执行,它们有时也可以按相反的顺序执行,这依所涉及的功能而定。也要注意的是,框图和/或流程图中的每个方框、

以及框图和/或流程图中的方框的组合,可以用执行规定的功能或动作的专用的基于硬件的系统来实现,或者可以用专用硬件与计算机指令的组合来实现。

[0089] 以上所述,仅为本申请的各种实施方式,但本申请的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本申请揭露的技术范围内,可轻易想到变化或替换,都应涵盖在本申请的保护范围之内。因此,本申请的保护范围应所述以权利要求的保护范围为准。

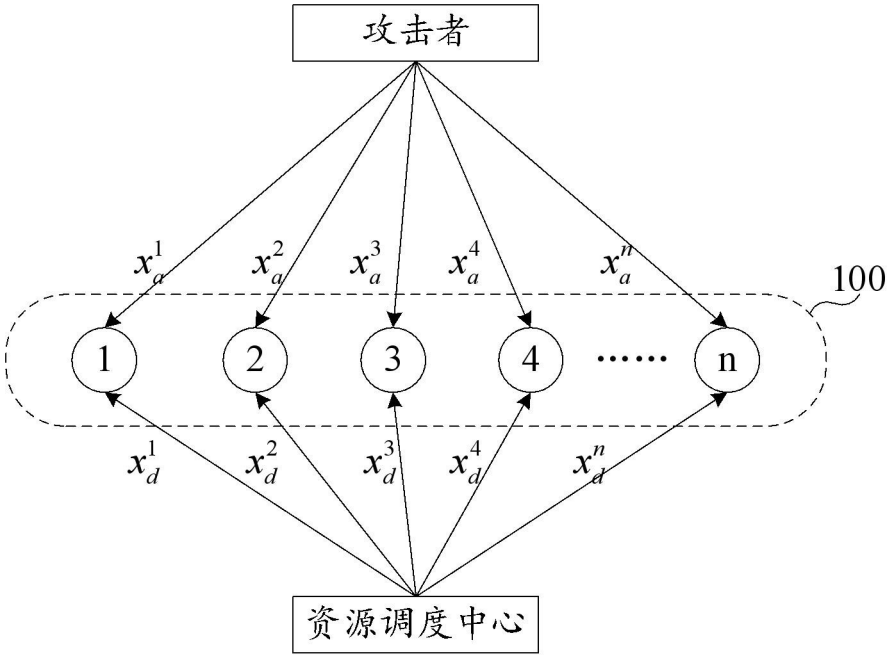

攻击者
x_a^1
x_a^2
x_a^3
x_a^4
x_a^n
100
1
2
3
4
……
n
x_d^1
x_d^2
x_d^3
x_d^4
x_d^n
资源调度中心

图1

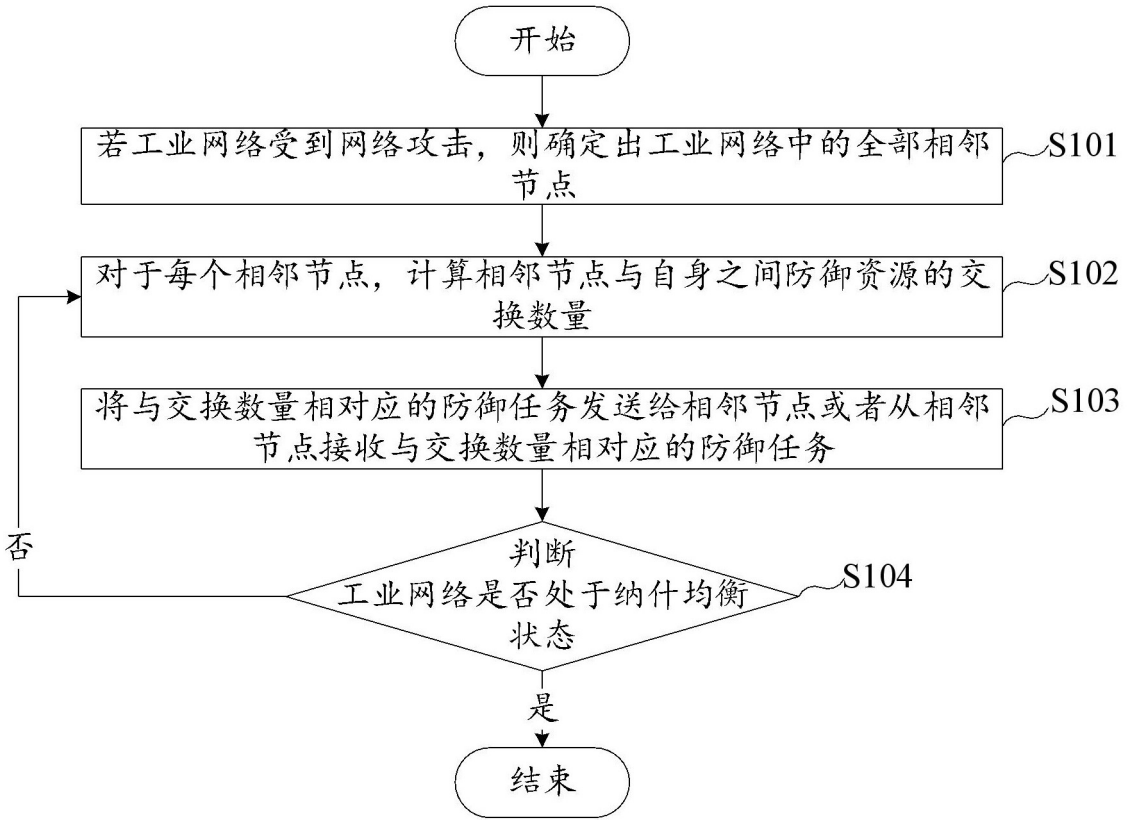

开始
若工业网络受到网络攻击，则确定出工业网络中的全部相邻节点
S101
对于每个相邻节点，计算相邻节点与自身之间防御资源的交换数量
S102
将与交换数量相对应的防御任务发送给相邻节点或者从相邻节点接收与交换数量相对应的防御任务
S103
判断工业网络是否处于纳什均衡状态
S104
否
是
结束

图2

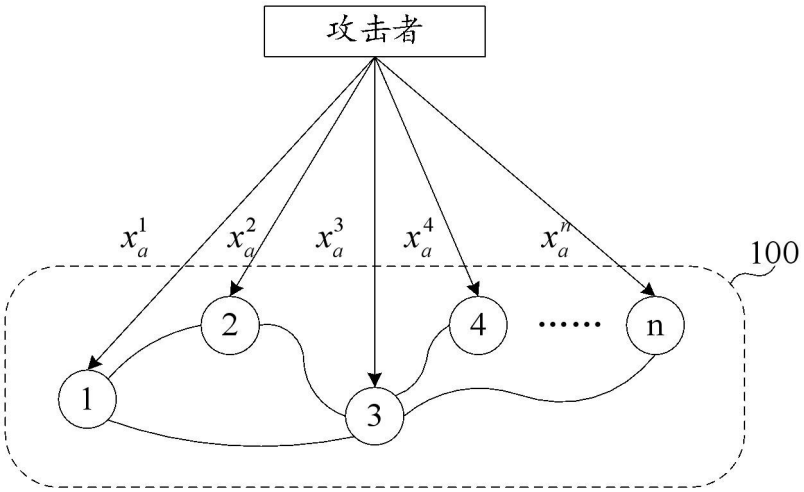

攻击者
x_a^1
x_a^2
x_a^3
x_a^4
x_a^n
100
1
2
3
4
n

图3

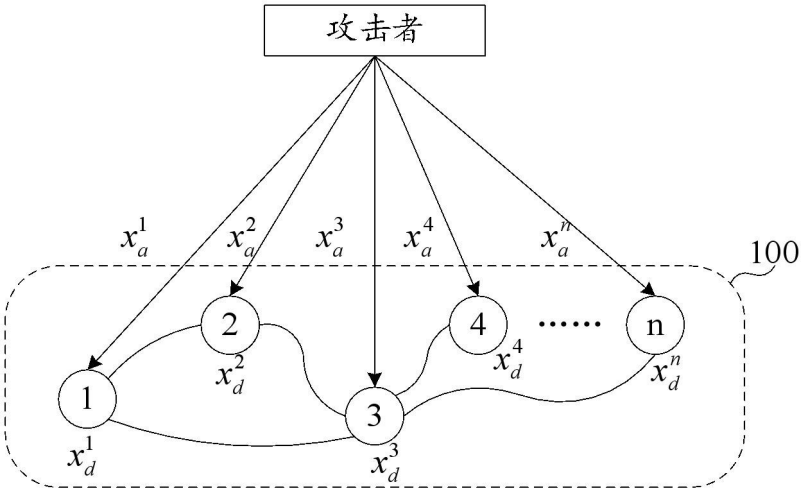

攻击者
x_a^1
x_a^2
x_a^3
x_a^4
x_a^n
100
1
2
3
4
n
x_d^1
x_d^2
x_d^3
x_d^4
x_d^n

图4

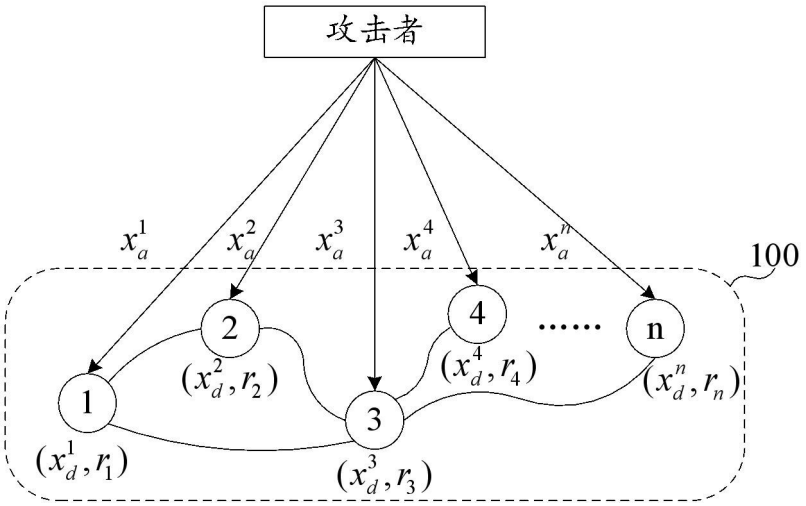

攻击者
x_a^1
x_a^2
x_a^3
x_a^4
x_a^n
100
1
2
3
4
n
.....
(x_d^1, r_1)
(x_d^2, r_2)
(x_d^3, r_3)
(x_d^4, r_4)
(x_d^n, r_n)

图5

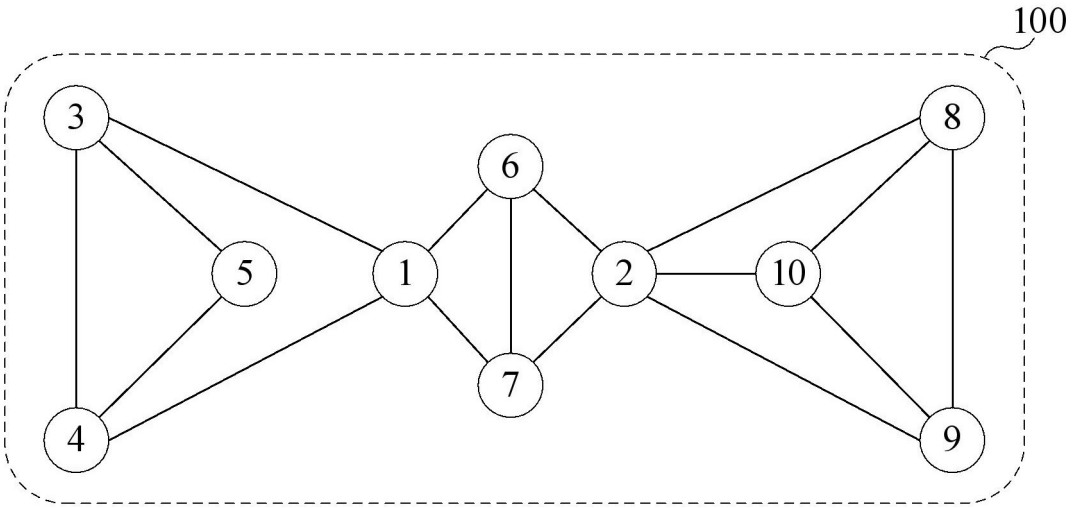

100
1
2
3
4
5
6
7
8
9
10

图6

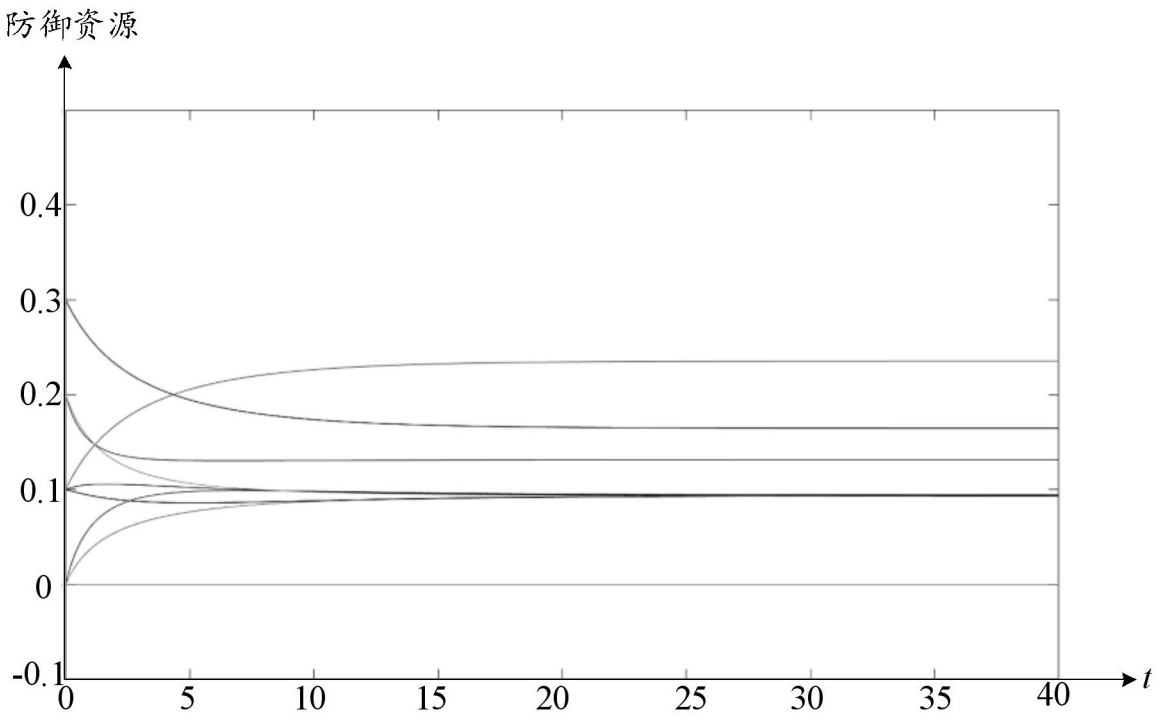


图7

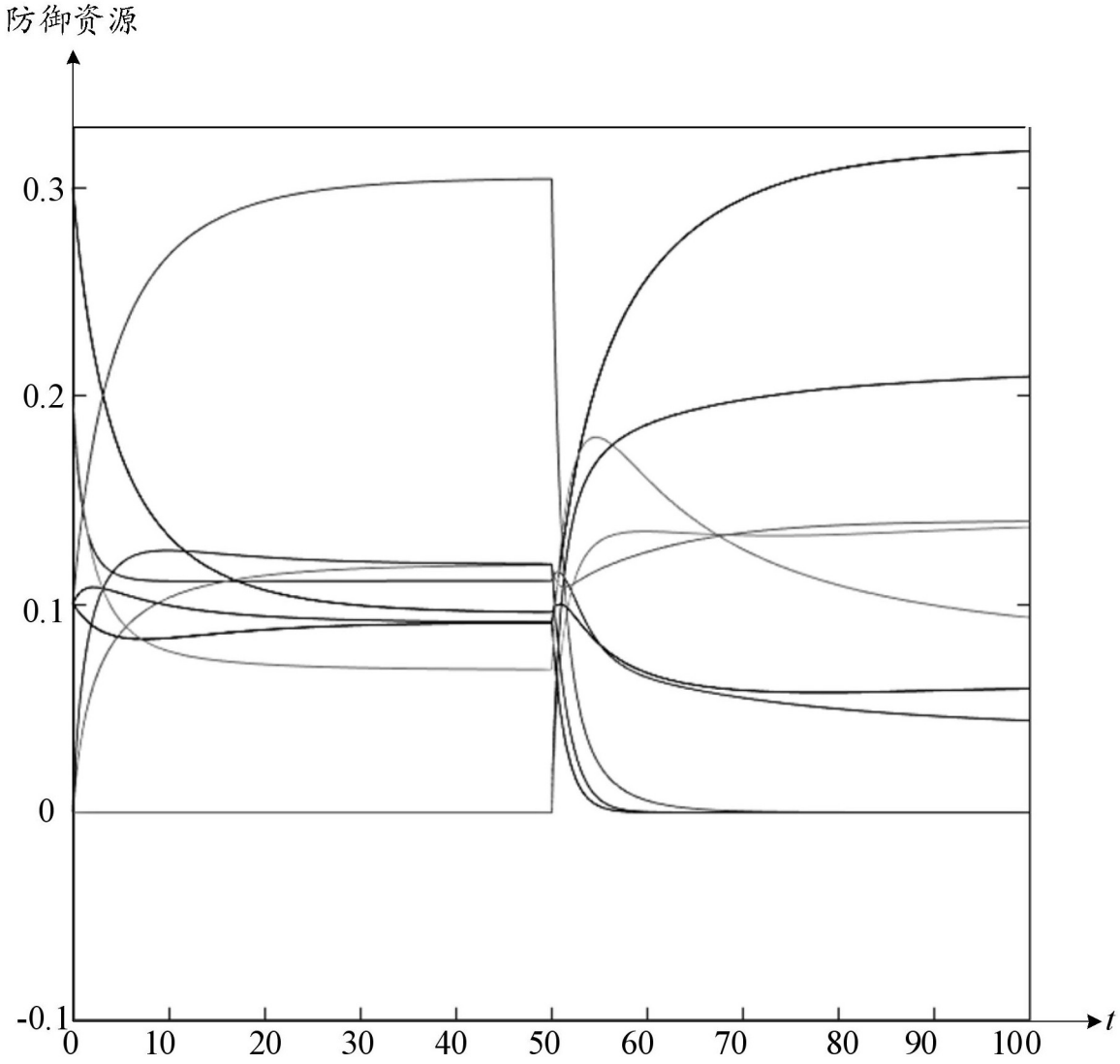

防御资源
0.3
0.2
0.1
0
-0.1
0
10
20
30
40
50
60
70
80
90
100
t

图8


相邻节点模块
201
资源交交互块
202
资源迭代模块
203

图9

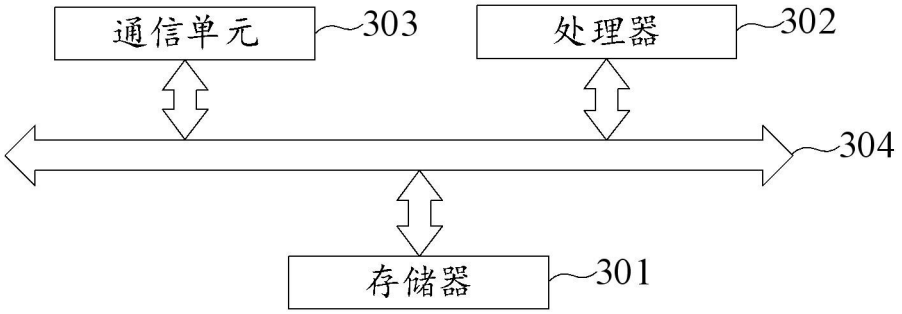


图10