文章编号：2095-2163(2023)07-0119-04 中图分类号：TP357 文献标志码：A

基于被动分簇算法的即时通信网络安全漏洞检测方法

张和伟，王奉章
（枣庄科技职业学院，山东 枣庄 277599）

摘 要：为了有效挖掘出网络协议漏洞，防止恶意攻击者泄露协议机密信息，维护协议运行环境安全，并改进安全漏洞检测技术，本研究提出了一种被动分簇算法在即时通信网络安全漏洞检测中的应用方法。首先，构建即时通信网络安全漏洞模型来界定监测区域，然后运用被动分簇算法获取即时通信网络节点。基于节点相对位置，用该算法确定安全弧序列以寻找节点漏洞弧段。随后，采用蚁群算法检测全部节点安全漏洞弧，从而实现完整安全漏洞的定位。仿真实验结果表明，本方法设计可精准检测即时通信网络安全漏洞节点，并且被动分簇算法在即时通信网络安全漏洞检测中的应用效果良好。因此，该方法对于挖掘和防范恶意攻击有着积极的作用，可以提高即时通信网络的安全性。

关键词：被动分簇算法；即时通信网络；安全漏洞；漏洞检测

A security vulnerability detection method for instant communication networks based on passive clustering algorithm

ZHANG Hewei, WANG Fengzhang
(ZaoZhuang Vocational College of Science and Technology, Zaozhuang Shandong 277599, China)

【Abstract】 In order to effectively discover network protocol vulnerabilities, prevent malicious attackers from leaking protocol confidential information, maintain the security of the protocol operating environment, and improve security vulnerability detection technology, this study proposes an application method of passive clustering algorithm in instant communication network security vulnerability detection. Firstly, construct an instant messaging network security vulnerability model to define the monitoring area, and then use passive clustering algorithm to obtain instant messaging network nodes. Based on the relative position of nodes, this algorithm is used to determine the sequence of security arcs to search for node vulnerability arcs. Subsequently, ant colony algorithm is used to detect all node security vulnerability arcs, thereby achieving the localization of complete security vulnerabilities. The simulation experimental results show that this method can accurately detect security vulnerability nodes in instant messaging networks, and the application effect of passive clustering algorithm in instant messaging network security vulnerability detection is good. Therefore, this method has a positive effect on mining and preventing malicious attacks, and can improve the security of instant messaging networks.

【Key words】 passive clustering algorithm; instant messaging network; security vulnerabilities; vulnerability detection

0 引 言

现如今，网络安全问题已引起社会高度关注，如黑客、病毒、木马等网络攻击手段，不仅可能直接牵涉到普通网民的个人隐私安全，也还会对信息的基础设施、物联网、大数据的安全等诸多领域产生重要影响，因而亟需采取全方位和多层次的防御手段，保障网络安全。

近年来，国内学术界在追求即时通信网络安全方面付出了巨大的努力，林若钦等学者[1]提出基于可变形卷积神经网络的软件漏洞检测算法，以可变形卷积神经网络为技术支持，设计一个漏洞检测方法，保障系统运行安全。马琪灿等学者[2]提出基于状态偏离分析的 Web 访问控制漏洞检测方法，将 Web 访问控制漏洞的检测转换为状态偏离的检测，降低了漏洞检测的误报率与漏报率。但是，由于即时通信网络本身具有一定的复杂性，且节点能量受限，上述方法在即时通信网络安全漏洞检测中均存在检测精准度不高的问题，所以仍无法避免即时通信网络漏洞的产生，恶意攻击者通过漏洞对即时通

作者简介：张和伟(1980-)，男，副教授，主要研究方向：计算机技术、计算机网络；王奉章(1974-)，男，讲师，主要研究方向：计算机技术、计算机网络。

收稿日期：2023-04-11

信网络进行访问或攻击,严重威胁着即时通信网络的运行安全。

为解决上述方法中存在的问题,研究设计了一种基于被动分簇算法的即时通信网络安全漏洞检测方法,基于被动分簇算法获取即时通信网络节点,根据节点相对位置确定安全弧序列,从而得到节点漏洞弧段,通过蚁群算法检测出全部节点安全漏洞弧,实现完整安全漏洞的定位。提高了漏洞检测的精准度,将即时通信网络安全漏洞的检测作为研究课题,旨在高效、全面地维护网络安全。

1 基于被动分簇算法的即时通信网络安全漏洞检测

被动分簇算法是一种基于被动感知的即时通信网络分簇算法,其原理是通过监听网络流量和节点之间的交互信息,自动识别和分类网络节点,将其归属到不同的簇中。该算法不需要节点主动加入或离开簇,而是通过感知节点之间的通信来实现簇的形成和维护。

1.1 构建即时通信网络安全漏洞模型

为了更好地检测即时通信网络安全漏洞,首先需要构建一个即时通信网络安全漏洞模型[3]。假设即时通信网络的特定区域内存在多个监测节点,且每一个节点随机部署于即时通信网络中,均处于静止不动的状态,一般情况下,各节点的最大通信半径为最大监测半径的 2 倍,以此为初始条件,构建一个即时通信网络安全漏洞模型,如图 1 所示。

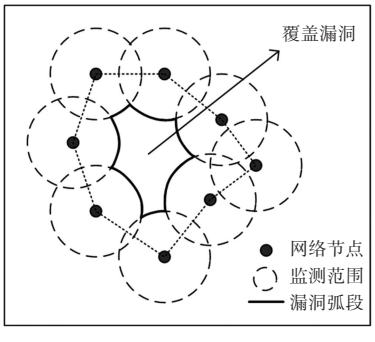

图 1 即时通信网络安全漏洞模型

Fig. 1 A security vulnerability model for instant communication networks

由图 1 可以看出,该模型利用一个圆形区域来表示即时通信网络的特定区域,其中有多个监测节点用小圆点表示,这些节点随机分布于该区域内,可以更好地定位即时通信网络中的安全漏洞,有效提高即时通信网络的安全性。如果想要检测即时通信网络安全漏洞所在位置,必须确定漏洞的最小周期循环,而最小周期循环主要由各节点的漏洞边缘弧段所构成。因此,在检测即时通信网络安全漏洞时,可以通过安全漏洞弧序列的检测来实现。

1.2 基于被动分簇算法的安全漏洞检测

当即时通信网络的节点失效,就会形成安全漏洞,然而失效节点的精确位置信息是未知的,所以在利用安全漏洞弧检测即时通信网络安全漏洞时,本文需要通过被动分簇算法来确定可能出现漏洞的即时通信网络节点[4-6]。在即时通信网络的簇内,如果网络节点失效,将无法再处理任何数据,需要通过中间节点进行信息传输,所以即时通信网络节点形成安全漏洞的概率为:

$$Q(x) = \eta S(x) \tag{1}$$

其中, $Q(x)$ 表示即时通信网络节点 x 变成失效节点的概率; η 表示比率系数; $S(x)$ 表示即时通信网络节点 x 映射范围内簇首数量。

在检测即时通信网络安全漏洞时可以通过漏洞弧段来实现,所以根据即时通信网络节点来确定安全漏洞弧序列[7]。由图 1 可知,即时通信网络节点为随机分布,在获得节点相对位置时,需要以节点为极坐标的极点,并将经过节点的射线当作极轴,即时通信网络节点的相对位置关系如图 2 所示。

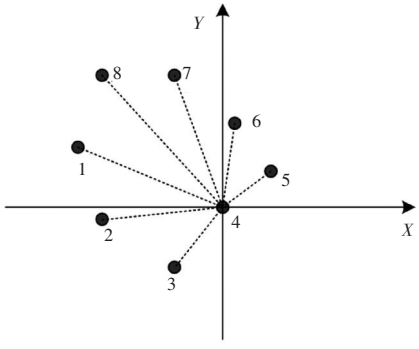

图 2 即时通信网络节点的相对位置关系

Fig. 2 The relative position relationship of instant messaging network nodes

由图 2 可知道,以节点 4 为例,首先将经过节点 4 的水平射线设为 X 轴,经过节点 4 的垂直射线设为 Y 轴,这样就可以获取节点 4 与其余邻近节点之间的距离,但仅依靠该距离无法直接确定各个节点的位置信息,所以本文通过虚拟移动准确得到各个节点之间的相对位置关系[8]。简单来说,就是将即时通信网络节点 4 沿着水平坐标轴,向另一个节点方向虚拟移动一定距离,此时,可以得到 2 个节点之间的另一条线段,与原始线段之间的夹角设为 ϑ,然后以同样的方法控制即时通信网络节点 4 沿着垂

直坐标轴，向节点方向虚拟移动一定距离，得到线段与原始线段之间的夹角为 ζ，如图 3 所示。

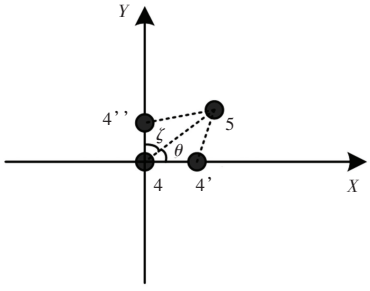

图 3　相邻网络节点的相对位置关系

Fig. 3　Relpositional relationships of adjacent network nodes

由图 3 可知，此时根据即时通信网络节点虚拟移动得到的 2 个虚拟节点，即可获取节点 4 与节点 5 的相对位置，假设节点 5 相对于节点 4 的位置信息为 $\langle d_1, \vartheta \rangle$，其中 d_1 为 2 个节点之间的相对距离，那么此时夹角 ϑ 与 ζ 满足如下关系：

$$\vartheta - \zeta = \frac{\pi}{2} \tag{2}$$

根据上述步骤即可求得各个即时通信网络节点的相对位置信息，在节点感知半径已知的情况下，根据式(3)可以计算出相邻 2 个节点的安全漏洞弧长：

$$L_{ij} = 2 \times \arccos\left(\frac{d_{ij}}{2 \times r}\right) \tag{3}$$

其中，L_{ij} 表示 2 个相邻即时通信网络节点 i 与 j 之间的安全漏洞弧长；d_{ij} 表示相邻即时通信网络节点 i 与 j 之间的相对距离；r 表示即时通信网络节点的感知半径。根据式(3)所求安全漏洞弧长，即可得到安全漏洞弧的方位角信息 $\langle \vartheta_{ij} - \frac{L_{ij}}{2}, \vartheta_{ij} + \frac{L_{ij}}{2} \rangle$。由图 1 可知，各相邻节点的监测范围存在相交现象，且每一个节点的 2 段安全漏洞弧也相交，所以各相邻两节点之间的距离不会超过即时通信网络节点感知半径的 2 倍，此时根据各节点之间的距离信息，即可确定即时通信网络节点被邻近节点所安全漏洞的弧序列，而未被邻近节点所安全漏洞的弧序列则为漏洞弧段，用于检测即时通信网络安全漏洞。

通过上述计算可以得到即时通信网络的、也就是漏洞弧段，在此基础上通过对各个边缘节点的遍历，即可得到全部的安全漏洞弧，以此实现即时通信网络安全漏洞检测[9]。本文引入蚁群算法来检测出即时通信网络节点的全部漏洞弧段信息，进而定位出即时通信网络的安全漏洞[10]。在蚁群搜索过程中，主要根据下面给出的概率公式来确定下一个遍历网络节点：

$$G_{uv}^{m}(t) = \frac{\alpha_{uv}(t)^{\varepsilon} \cdot (B_v)^{\omega} \cdot l_{uv}(t)^{\zeta}}{\sum_{z \in Y_u} \alpha_{uz}(t)^{\varepsilon} \cdot (B_z)^{\omega} \cdot l_{uz}(t)^{\zeta}}, \quad z \in Y_u \tag{4}$$

其中，$G_{uv}^{m}(t)$ 表示 t 时刻蚂蚁 m 由即时通信网络节点 u 转移至节点 v 的概率；α_{uv} 表示即时通信网络节点 u 与 v 之间路径上的信息素浓度；l_{uv} 表示即时通信网络节点 u 与 v 之间的直线距离；B_z 表示即时通信网络节点 u 的邻近节点 z 的标签值；ε 表示蚁群信息素的加权因子；ω 表示节点标签值的加权因子；ζ 表示节点 u 与 v 之间直线距离的加权因子；Y_u 表示即时通信网络节点 u 的邻近节点中未被蚁群遍历过的节点集合。一般情况下，蚁群在搜索即时通信网络节点安全漏洞弧时，会根据节点的标签值来选取下一个遍历节点，也就是节点标签值越大，其被遍历的可能性越大。与此同时，在蚁群搜索即时通信网络节点安全漏洞弧的过程中，会根据信息素浓度的变化来定位安全漏洞的位置，其表达式如下：

$$\alpha_{uv}(t+1) = (1-\rho)\,\alpha_{uv}(t) + N \tag{5}$$

其中，ρ 表示蚂蚁信息素的挥发系数；N 表示即时通信网络节点 u 与 v 之间路径上的信息素增量。在蚁群遍历即时通信网络节点的过程中，所搜索到的信息素浓度较高的节点，会形成一个最小周期环，也就是全部安全漏洞弧段，所以等到全部蚂蚁遍历即时通信网络节点完毕之后，就可以定位出完整安全漏洞的位置，从而实现即时通信网络安全漏洞的检测。

2　仿真实验

在 Matlab 软件中，随机部署一个即时通信网络进行仿真，其具体的实验参数布置见表 1。

表 1　实验参数设置

Tab. 1　Experimental parameter settings

项目	参数
网络模拟范围	200 m * 200 m 的矩形区域
网络节点/个	120
节点感知半径/m	20
节点通信半径/m	40

以表 1 的数据作为研究基础，以基于可变形卷积神经网络的即时通信网络安全漏洞检测方法[1]、基于状态偏离分析的即时通信网络安全漏洞检测方法[2]作为对照组，与本文设计方法一起进行对比实验，并根据对比结果来判断本文方法是否可行。

由于本文将被动分簇算法应用于即时通信网络安全漏洞检测时,主要是在网络节点的位置信息上进行的,所以本次仿真实验过程中在 200 m * 200 m 的矩形区域内,随机部署 10、20、30、50、80、100 个漏洞节点,形成 6 个安全漏洞检测场景,在每一个场景下分别执行上述 3 种检测方法,并统计各方法的检测准确率。即时通信网络安全漏洞检测对比结果如图 4 所示。

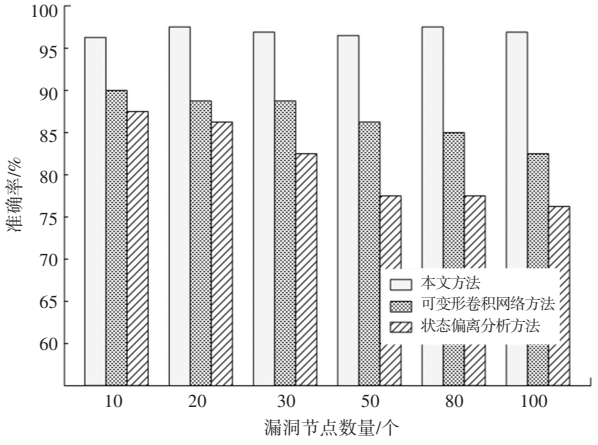

图 4 即时通信网络安全漏洞检测结果对比图

Fig. 4 Comparison of instant messaging network security vulnerability detection results

由图 4 可知,随着即时通信网络安全漏洞节点数量的增加,可变形卷积网络与状态偏离分析方法下的检测准确率呈下降趋势,而本文设计方法下的检测准确率整体处于较为稳定的状态。在上述 6 个即时通信网络安全漏洞检测场景中,本文设计方法的检测准确率的平均值为 96.9%,较实验对照组方法分别提高了 10.1%、15.6%,由此可以说明本文设计方法更具优越性,验证了被动分簇算法在即时通信网络安全漏洞检测中应用效果良好。

为了进一步验证本文方法的可行性,选取即时通信网络安全漏洞检测耗时作为指标,采用基于可变形卷积神经网络的即时通信网络安全漏洞检测方法[1]、基于状态偏离分析的即时通信网络安全漏洞检测方法[2]以及本文方法对即时通信网络安全漏洞进行检测,对比其检测效率,其检测耗时越短、效率越高。对比结果见表 2。

分析表 2 可知,与 2 种现有方法相比,本文方法的耗时仅需20 s,实现了大幅度的降低。可以得出该方法可以更快速、更准确地检测出即时通信网络中的安全漏洞,从而提高即时通信网络的安全性。

表 2 3 种方法作用下网络安全漏洞检测的耗时对比

Tab. 2 Time-consuming comparison of network security vulnerability detection under the action of the three methods

	本文方法	可变形卷积神经网络方法	状态偏离分析方法
检测耗时/s	20	45	60

3 结束语

本文结合被动分簇算法,针对即时通信网络安全漏洞检测问题进行了深入研究和创新性工作,在文中所设计即时通信网络安全漏洞检测方法中,依赖于网络节点与安全漏洞弧,采用被动分簇算法完成安全漏洞弧的计算后,利用蚁群算法实现安全漏洞的检测,并通过仿真实验验证了本文设计即时通信网络安全漏洞检测方法的可行性与可靠性。虽然本文已经取得一定研究成果,但在即时通信网络安全漏洞检测过程中,易发生边界节点过早死亡的现象,所以未来将针对漏洞边界节点的调度方法做进一步的研究,以此延长即时通信网络的生命周期,推动即时通信网络可持续发展。

参考文献

[1] 林若钦,罗琼. 基于可变形卷积神经网络的软件漏洞检测算法[J]. 计算机仿真,2021,38(03):405-409.
[2] 马琪灿,武泽慧,王允超,等. 基于状态偏离分析的 Web 访问控制漏洞检测方法[J]. 计算机科学,2023,50(02):346-352.
[3] 文敏,王荣存,姜淑娟. 基于关系图卷积网络的源代码漏洞检测[J]. 计算机应用,2022,42(06):1814-1821.
[4] 李明磊,黄晖,陆余良,等. SymFuzz:一种复杂路径条件下的漏洞检测技术[J]. 计算机科学,2021,48(05):25-31.
[5] 张杰,景雯,陈富. 基于被动分簇算法的即时通信网络协议漏洞检测[J]. 吉林大学学报(工学版),2021,51(06):2253-2258.
[6] 李威,姜学峰,李健俊,等. 面向工业计算机的网络入侵行为检测[J]. 计算机应用,2022,42(S1):178-183.
[7] 管军霖,师功才,陈宏. 基于 Apriori 风险数据分析的网络漏洞挖掘研究[J]. 计算机仿真,2022,39(01):343-347.
[8] 杨宏宇,杨海云,张良,等. 基于特征依赖图的源代码漏洞检测方法[J]. 通信学报,2023,44(01):103-117.
[9] 许健,陈平华,熊建斌. 基于抽象内存模型的内存相关漏洞检测方法[J]. 计算机工程与应用,2022,58(08):96-108.
[10] 陈亮,李永刚,刘磊,等. 基于特征的电力信息系统注入漏洞检测方法[J]. 计算机工程与设计,2021,42(08):2115-2123.