**密级： 保密期限：**

xm 拷贝

**硕士学位论文**



**题目： 基于机器学习的威胁情报**

**可信分析系统的研究**

**学 号： 2016110991**

**姓 名： 程翔龙**

**专 业： 软件工程**

**导 师： 李小勇**

**学 院： 软件学院**

**年 月 日**

独创性（或创新性）声明

本人声明所呈交的论文是本人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢中所罗列的内容以外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得北京邮电大学或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

申请学位论文与资料若有不实之处，本人承担一切相关责任。

本人签名： 日期：

关于论文使用授权的说明

本人完全了解并同意北京邮电大学有关保留、使用学位论文的规定，即：北京邮电大学拥有以下关于学位论文的无偿使用权，具体包括：学校有权保留并向国家有关部门或机构送交学位论文，有权允许学位论文被查阅和借阅；学校可以公布学位论文的全部或部分内容，有权允许采用影印、缩印或其它复制手段保存、汇编学位论文，将学位论文的全部或部分内容编入有关数据库进行检索。（保密的学位论文在解密后遵守此规定）

本人签名： 日期：

导师签名： 日期：

**基于机器学习威胁情报可信分析系统的研究**

**摘 要**

近些年来，随着信息技术的飞速进步与发展，网络安全技术不断演化，无论是以5G通讯，物联网等新型网络形式的出现，还是以在线社交网络等为代表的新型服务模式的出现，都不断呈现出开放性、异构性、移动性和可信性的特点，这些服务方便了人们的生活，但是由于网络的匿名性，人们同时也遭受着非法网络渗透等带来的巨大损失和伤害。针对日益庞大的网络用户的威胁情报数据，如何对这些威胁情报进行合理的分析和研究将成为新时代下社会信任体系与主动安全防御的重中之重。

现今的互联网环境下，人们对用户实体的威胁情报数据的主要来源就是网络，尤其是大规模的在线社交网络，但是社交网络中的威胁情报数据具有匿名性，同时具有数据规模大，关联关系复杂等特点，如何有效的对这些用户实体的威胁情报数据进行高效并且合理的研究与利用，是解决网络空间环境下，对网络用户的威胁情报进行信任评估的关键。

因此，本文主要针对大规模在线社交网络环境中的威胁情报的信任评估问题进行研究，主要的工作任务如下：

（1）针对大规模网络环境中，威胁情报数据规模大、关联关系复杂的特点，本文提出了一种基于机器学习方法的海量数据知识图谱构建的方法。该方法利用网络空间中威胁情报数据的结构化和非结构化特性，对原始的威胁情报数据进行实体、属性和关系的抽取；考虑抽取得到的实体、属性和关系信息之间存在重复、别名问题，再利用知识融合的技术对抽取得到的实体、属性和关系进行加工、整合、消除歧义；最后，针对得到的实体别名不一致或者冲突的问题，本文采用二分类的机器学习方法来消除异构实体数据存在的冲突问题。这样，就可以得到一系列基于事实表达的高质量的威胁情报知识图谱，构建的威胁情报知识图谱质量越高，将使得基于知识图谱的信任评估计算越精确。

（2）针对网络环境中用户情报数据中质量低和虚假数据的问题，本文提出了一种基于知识图谱的用户情报数据的信任评估模型。该模型首先利用知识表示TransE（Translating Embeddings）算法威胁情报知识图谱中的实体、属性和关系等节点信息映射成低维向量空间的向量；为了计算两个节点之间的信任关系，我们提出一种基于循环神经网络（Recurrent Neural Network, RNN）的路径聚合算法来计算得到两个节点之间任意一条路径的信任数值，然后通过路径可靠性算法（Path Reliability Measuring Algorithm，PRM）对两节点之间存在的多条关系路径进行信任关系的加权计算，实验结果表明，基于上述的威胁情报信任评估模型，相较于传统的基于规则运算的模型，具有较高的准确度。

（3）针对现实网络环境中的用户信任评估的需求，本文基于新浪微博，设计并且实现了一套新浪微博用户情报数据的可信评估系统。该系统分为威胁情报数据爬取模块、威胁情报数据预处理模块、威胁情报知识图谱构建模块、威胁情报可信分析模块。其中情报数据爬取模块利用网络爬虫对新浪微博的用户情报数据进行爬取；威胁情报数据预处理模块旨在对原始的结构化威胁情报数据进行实体、属性和关系的解析；威胁情报知识图谱构建模块利用获取到的威胁情报数据，利用知识图谱的构建方法，构建高质量的威胁情报知识图谱；威胁情报信任分析模块将利用上述路径聚合算法和路径可靠性算法对威胁情报进行信任关系的可信评估；最后，系统额外提供可视化平台用户对构建的知识图谱进行可视化展示。

**关键词：**威胁情报 知识图谱 机器学习 信任评估

**STUDY ON TRUSTWORTHY ANALYSIS OF THREAT INTELLIGENCE BASED ON MACHINE LEARNING**

**ABSTRACT**

In recent years, with the rapid advancement and development of information technology, network security technology has evolved. Whether it is the emergence of new types of networks such as 5G communication and Internet of Things, or the emergence of new service models such as online social networks, they are constantly showing the characteristics of openness, heterogeneity, mobility and credibility. These services are convenient for people's lives, but due to the anonymity of the network, people also suffer huge losses and injuries caused by illegal network penetration. Aiming at the threat intelligence data of the increasingly large network users, how to conduct reasonable analysis and research on these threat intelligences will become the top priority of the social trust system and active security defense in the new era.

In today's Internet environment, the main source of threat intelligence data for user entities is the network, especially large-scale online social networks, but the threat intelligence data in social networks is anonymized, and the data size is large and the relationship is complicated. Due to those characteristics, how to effectively and effectively research and utilize the threat intelligence data of these user entities is the key to solving the trust evaluation of threat information of network users in the cyberspace environment.

Therefore, this paper focuses on the trust assessment of threat intelligence in large-scale online social network environment. The main tasks are as follows:

(1) Aiming at the large-scale online social network environment, due to the threat intelligence data is large in scale and complex in relation, this paper proposes a method based on machine learning for constructing massive knowledge graph of the threat intelligence. The method utilizes the structured and unstructured characteristics of threat intelligence data in cyberspace to extract the entities, attributes and relationships of the original threat intelligence data. Considering the existence of duplicates and aliases between extracted entities, attributes, and relationship information, and then using knowledge fusion techniques to process, integrate, and disambiguate the extracted entities, attributes, and relationships. Finally, in view of the inconsistent or conflicting problem of the obtained entity aliases, this paper uses the two-class machine learning method to eliminate the conflict of heterogeneous entity data. In this way, a series of high-quality threat intelligence knowledge maps based on facts can be obtained. The higher the quality of the constructed threat intelligence knowledge graph, the more accurate the trust evaluation calculation based on the knowledge graph.

(2) Aiming at the anonymity of user intelligence data in network environment, this paper proposes a trust evaluation model based on knowledge graph of user intelligence data. The model uses the TransE (Translating Embeddings) algorithm to map the information of entities, attributes and relationships in the intelligence knowledge graph to the vector of low-dimensional vector space. In order to calculate the trust relationship between two nodes in two knowledge graph, we propose a path aggregation algorithm based on Recurrent Neural Network (RNN) to calculate the trust value of any path between two nodes. Then, through the Path Reliability Measuring Algorithm (PRM), the weighted calculation of the final trust relationship with multiple relationship paths between the two nodes is carried out. The experimental results show that the above-mentioned threat intelligence trust evaluation model has higher accuracy than the traditional rule-based operation model.

(3) Aiming at the needs of user trust evaluation in real network environment, this paper designs and implements a trust evaluation system based on user intelligence data of Sina Weibo. The system is divided into threat intelligence data crawling module, threat intelligence data preprocessing module, threat intelligence knowledge graph building module, threat intelligence credibility analysis module. The intelligence data crawling module uses the web crawler to crawl the user intelligence data of Sina Weibo; the threat intelligence data preprocessing module aims to analyze the entities, attributes and relationships of the original structured threat intelligence data; The threat intelligence knowledge graph construction module uses the acquired threat intelligence data to construct a high-quality threat intelligence knowledge graph by using the knowledge graph construction method; the threat intelligence trust analysis module uses the path aggregation algorithm and the path reliability algorithm mentioned above is used for trust evaluation. Finally, the system provides a visual platform to visually display the constructed knowledge graph.

**KEY WORDS:** Threat Intelligence; Knowledge Graph; Machine Learning; Trust Evaluation

**目 录**

[第一章 绪论 1](#_Toc477870353)

[1.1 本模板发布简介 1](#_Toc477870354)

[1.2 作者信息 1](#_Toc477870358)

[第二章 测试 3](#_Toc477870359)

[2.1 测试环境 3](#_Toc477870360)

[2.2 测试方法 3](#_Toc477870361)

[第三章 TEST 5](#_Toc477870362)

[参考文献 6](#_Toc477870363)

[致谢 7](#_Toc477870364)

[攻读学位期间取得的研究成果 8](#_Toc477870365)

1. 绪论
   1. 研究背景

随着信息技术的飞速发展，以社交网络、电子商务为代表的新的互联网服务模式的出现与快速发展，极大的便捷了人们的日常生活，使得人与人的交流可以跨越地域的鸿沟，更加方便快捷的与人沟通。而无论是电子商务，亦或是社交网络，这些互联网新型服务模式无不有着开放性、移动性、异构型以及匿名性的特点。最新发布的中国互联网络发展状况统计报告显示，截至到2018年12月，中国的互联网用户规模已经突破8亿，互联网的普及率接近60%。我们不得不认识到网络已经成为人们进行衣食住行、人际交流等人类社会活动的重要渠道，更为重要的事，由于网络的匿名以及开放特性，也给了犯罪分子实施网络犯罪的可趁之机。中国互联网信息中心（China Internet Network Information Center, CNNIC）研究报告指出，中国有近一半的互联网用户都曾遭遇过网络犯罪的侵害，其中“虚拟中奖信息诈骗”占受害网民总数的比例最高，其次是“冒充好友诈骗”和“网络兼职诈骗”。因此，以社交网络以及电子商务为代表的新型互联网环境下的安全问题已经成为严重的社会问题，严重危害到人们的生命财产安全，甚至跨国的、有组织的网络犯罪将对中国国家安全造成严重的威胁。

网络环境的开放性和匿名性为犯罪分子实施危害人们生命财产安全，甚至危害国家安全的犯罪活动提供便捷的犯罪工具，而且由于网络的加密通信和移动性，也加大了国家安全部门的执法难度，非法的网络犯罪活动将给人们和国家造成无法挽回的损失。2018年9月，中央电视台焦点访谈节目播出了有关台湾间谍的专题节目，纰漏了台湾间谍通过伪造身份，对祖国大陆肆意进行渗透，组织非法犯罪活动，严重危害中国国家两岸关系的和平发展以及中国大陆的国家安全。同样，在2018年上映的电影“网络迷踪”中，男主角大卫的女儿玛戈突然失踪，前来调查该案件的女警官曾声称玛戈可能只是离家出走，并且在案件调查过程中制造玛戈被杀害的假象，大卫通过该警官的社交网络状态，经过一步步的细心分析思考，识破了案件过程中相关人物的真实身份，发现女警官并不是来帮助自己的，最后经过仔细分析研究玛戈的网络账号情报数据，成功解救了玛戈。由此可见，在当今的网络环境下，安全问题依然是亟待解决的关键，并且大卫解救玛戈的故事也给我们防御网络环境中的网络犯罪提供了新的思路。

因此，在以社交网络为代表的新的快速发展的网络环境中，如何有效的防御网络犯罪，需要解决以下问题：

（1）如何快速有效的从海量的、零散的网络数据中挖掘出有价值的情报数据；

（2）如何为海量的、零散的情报数据建立合适的关联关系模型；

（3）如何在海量的情报关系数据中识别虚假的情报，为情报数据进行信任评估。

当下，在充满安全威胁的网络环境中，为了解决上述的问题，基于知识图谱表示的威胁情报应运而生。威胁情报作为新的网络环境下情报数据的收集、整合和评估，来帮助网络安全的从业人员主动防御可能发生的安全威胁的直接手段，因此不管从个人安全角度还是国家安全角度来说，威胁情报都受到了足够的重视。当人们需要与未知的陌生用户进行交互的时候，可以通过该陌生用户在网络环境中的威胁情报数据对该用户进行快速精确的可信评估，国家安全部门可以利用威胁情报数据，快速精准的分析出未知用户的真实身份特性，进行采取主动防御措施。因此，威胁情报为新型网络服务环境下人民和国家的安全提供了强有力的安全保障。但是，威胁情报本身的一些特性也导致需要迫切的解决以下问题：

（1）威胁情报数据规模大，关联关系分散

在当今网络飞速发展的时代，每天都会产生巨大的威胁情报数据，这些情报数据分散在网络环境中的各个位置，如何有效的组织这些威胁情报数据将面临着巨大的挑战。而且，分散着的威胁情报中包含了无数的实体信息，这些实体之间或多或少的存在着关联关系，但是由于威胁情报数据的分散性，导致这些关联关系难以观察，对有效利用威胁情报产生的巨大的阻碍。因此，如何有效的组织威胁情报，并且为威胁情报中的实体建立关联关系将成为我们首先需要解决的问题。

（2）存在低质量、虚假的威胁情报

由于网络环境的开放性和匿名性，通过网络环境收集的威胁情报中充斥着大量的质量低的、虚假的情报信息，这些情报信息的存在将严重污染威胁感知计算的数据来源，对最终的计算和预测结果造成严重干扰，海量的威胁情报中真正有价值的威胁情报数据沧海一粟，具有有效威胁情报数据价值密度低的特性。因此，根据收集的威胁情报进行安全威胁预测和计算的前提是能主动识别出哪些威胁情报数据是可信的，哪些是不可信的。

（3）复杂的威胁情报数据难以加以利用

正如上文中提到的威胁情报具有数据规模大的特性，传统的计算方法难以对规模如此巨大的威胁情报数据进行分析研究，更不用说主动识别真正有价值的、有效的、真实的威胁情报数据。因此，如何使用有效的技术手段对海量的威胁情报数据进行信任分析将成为威胁情报能被有效利用的关键问题。

基于上文所提到的关键性问题，高效的威胁情报的信任评估是提高人民和国家的网络危险状态识别和主动安全防御能力，保障人民生命财产安全和国家安全的重要技术保障。因此，应用知识图谱构建的技术构建威胁情报知识图谱，并应用先进的机器学习算法对威胁情报进行信任分析是本文研究的主要目标，这也必将成为未来威胁情报分析的主要手段。

* 1. 国内外研究现状

Xxx

* 1. 研究内容

根据上文所述，本文主要以威胁情报研究中存在的数据规模大、关联关系分散，存在低质量、虚假的威胁情报以及复杂的威胁情报数据难以加以利用的问题为出发点，应用机器学习算法对威胁情报进行信任评估。传统的威胁情报信任分析的方法主要有组合证据理论和传统的规则计算的方式，并且几乎没有人考虑威胁情报数据的组织方式。例如：在对情报信息本身进行信任分析时，信任分析工作的主要是以情报内容的超链接关系以及情报本身的上下文内容来建立模型；在对用户进行信任评估的时候，主要是基于投票和关系传播的方式来建立模型，并且模型计算的方式主要采用简单的规则运算；在对信息源进行信任评估的时候，主要是以网站本身的访问量、网站本身的结构以及网站之间的链接关系来建立模型。在传统的研究方法中，主要是从信任分析的目标出发，向外扩散，构建目标的局部关联范围，因为这些方式只考虑局部的威胁情报价值，而没有对全局的威胁情报加以利用，这样最终得到的结果就没法保证其完备性和准确性。因此，本文主要的研究内容包含以下几个方面：

（1）构建威胁情报的知识图谱

威胁情报具有数据规模大，关联关系复杂等特点，难以直接有效的利用。而知识图谱可以利用机器学习等核心技术对原始的威胁情报进行知识抽取，得到威胁情报中隐含的实体、属性以及关系，并建立实体与实体、实体与属性之间的三元组关系。在知识图谱中，每个实体和属性都是一个节点，这些节点之间通过关系建立连接，因此在海量数据检索方面具有得天独厚的优势。

（2）研究威胁情报信任评估的方法

以威胁情报知识图谱为依托，利用TransE算法将威胁情报知识图谱三元组中的实体、关系和属性映射成低维向量空间中的向量，然后利用基于RNN的路径关系聚合算法和关系路径可靠性算法对实体与实体、实体与属性之间的关系进行可信评估。

（3）研究威胁情报信任分析系统的应用

设计并且实现了一套新浪微博的社交网络用户威胁情报数据的信任评估系统。该系统以新浪微博为威胁情报数据来源，采用分布式网络爬虫获取原始的威胁情报数据，并利用自然语言处理等机器学习技术对获取的原始情报进行知识抽取，构建威胁情报知识图谱；在此基础上，以基于TransE和RNN为核心的威胁情报信任评估算法为主要模块构建威胁情报信任评估系统，并对外提供用户使用的接口API。另外，基于知识图谱可视化技术，提供用户查询知识图谱的可视化平台。

根据上文所描述的主要研究内容，本文的主要研究特点总结如下：

（1）使用知识图谱作为威胁情报表示和分析应用的基础

知识图谱是大数据和人工智能时代的产物，其三元组形式的表示结构可以清晰的展示节点之间的关联关系，而威胁情报的主要任务就在于情报数据的收集，语义理解以及关联关系建立，这与知识图谱的优势不谋而合，正是这样，本文采用知识图谱作为威胁情报表示和分析应用的基础.

（2）采用RNN来作为威胁情报信任评估算法的核心

RNN。。。。

（3）设计并实现了基于新浪微博的威胁情报信任评估系统

系统以新浪微博为威胁情报数据的来源，通过Flask这一轻量级的Python Web开发框架进行迭代开发，通过分布式网络爬虫获取原始的微博情报数据，利用自然语言处理对情报数据进行知识抽取，构建知识图谱，并通过先进的前端可视化技术对构建的知识图谱进行直观展示。系统以TransE和RNN为核心构建威胁情报信任分析算法的模型，提高了判别的准确性。

* 1. 论文组织

本文共分为五章展开叙述，具有章节的组织方式如下：

第一章 绪论。本部分首先介绍以社交网络等为代表的开放的互联网环境下存在的安全威胁，由此引出威胁情报产生的背景，重点阐述了威胁情报研究存在主要问题和难点；接着对国内外的研究现状进行了介绍，表明亟待解决的问题以及相应的研究内容，并在此基本上提炼了本文的主要工作内容；最后介绍了本文的组织方式。

第二章 威胁情报和信任评估的相关研究。本部分首先从威胁情报自身特性出发，详细介绍了威胁情报的主要特点以及需要解决的问题，并详细阐述了威胁情报领域的信任评估机制的研究工作；接着对信任以及信任评估进行了详细的说明，并总结了信任的特点以及主要的信任分析的模型。

第三章 威胁情报信任分析模型的研究。首先介绍了开放网络环境下威胁情报研究的主要思路，然后引入以机器学习算法为核心的威胁情报知识图谱，并以此作为威胁情报信任分析的基础。以TransE算法为核心将威胁情报知识图谱的实体、属性以及关系节点映射到低维向量空间，在此基础上，引入以RNN为核心的威胁情报信任分析算法。本章首先介绍了知识图谱的主要理论以及其在威胁情报领域的应用价值，然后介绍了TransE算法和RNN算法的主要理论知识，详细分析了模型的特点和计算方式，并给出部分模型计算的源代码，最后在数据集的基础上，通过与传统的信任评估算法对比，对模型的性能进行了评价。

第四章 威胁情报信任分析原型系统的设计与实现。本章首先对威胁情报信任分析平台的用户需求进行了分析，然后设计系统开发的总体架构，接着详细的阐述了系统中各个模块的主要功能，以及设计与实现方式，最后从功能角度完成系统的测试。

第五章 总结与展望。本章主要总结全文的研究成果，并在此基础上分析暂时存在的问题，以及接下来需要继续进行的工作，展望未来的工作。

论文的主要组织架构方式如图1-1所示：

1. 威胁情报和信任评估的相关研究
   1. 威胁情报的研究工作
      1. 威胁情报的主要特点
      2. 威胁情报的信任分析
   2. 信任评估的研究工作
      1. 信任评估中的相关定义
      2. 信任评估的典型应用场景
      3. 信任评估的理论模型
   3. 本章小结
2. 威胁情报信任分析模型的研究
   1. 威胁情报信任分析的研究思路
   2. 基于知识图谱的威胁情报知识表示模型
      1. 知识图谱的原理
      2. 基于知识图谱的威胁情报知识表示算法
   3. 基于RNN的威胁情报信任分析模型
      1. 循环神经网络RNN算法
      2. 基于RNN的威胁情报信任分析算法
   4. 本章小结
3. 威胁情报信任分析原型系统的设计与实现
   1. 威胁情报信任分析的需求分析
      1. 威胁情报信任分析的需求背景
      2. 威胁情报信任分析的功能需求
   2. 威胁情报信任分析系统的架构设计
      1. 威胁情报信任分析系统的功能结构
      2. 威胁情报信任分析系统的架构设计
   3. 威胁情报信任分析系统核心模块的设计与实现
      1. 关键技术
      2. Xxx
      3. xxx
      4. xxx
   4. 系统功能测试与结果
      1. 测试环境
      2. 原型系统的功能测试
   5. 本章小结
4. 总结与展望
   1. 全文总结
   2. 下一步工作

参考文献

致谢

感谢CCTV!

攻读学位期间取得的研究成果