·网络空间安全· 文章编号:1000-3428(2021)03-0139-08 文献标志码:A 中图分类号:TP309

一种基于攻击树的4G网络安全风险评估方法

王赛娥,刘彩霞,刘树新,柏 溢
(中国人民解放军战略支援部队信息工程大学,郑州 450001)

摘 要: 针对4G网络的安全风险评估问题,提出一种基于攻击树模型的评估方法,以分析网络的风险状况,评估系统的风险程度和安全等级。对4G网络的安全威胁进行分类,通过梳理攻击行为和分解攻击流程来构造攻击树模型,利用多属性理论赋予叶节点3个安全属性并通过等级评分进行量化,结合模糊层次分析法和模糊矩阵计算叶节点的风险概率,根据节点间的依赖关系得到根节点的风险概率,最终得到4G网络的安全风险等级。实验结果表明,该方法能够准确评估4G网络的风险因素,预测可能的攻击路径,为安全防护策略选择提供依据。

关键词: 4G网络;安全威胁;攻击树模型;风险评估;模糊层次分析法

开放科学(资源服务)标志码(OSID):

中文引用格式: 王赛娥,刘彩霞,刘树新,等.一种基于攻击树的4G网络安全风险评估方法[J].计算机工程,2021,47(3):139-146,154.

英文引用格式: WANG Saie,LIU Caixia,LIU Shuxin,et al.A method of 4G network security risk assessment based on attack tree[J].Computer Engineering,2021,47(3):139-146,154.

A Method of 4G Network Security Risk Assessment Based on Attack Tree

WANG Saie,LIU Caixia,LIU Shuxin,BAI Yi
(People's Liberation Army Strategic Support Force Information Engineering University,Zhengzhou 450001,China)

【Abstract】 This paper proposes a security risk evaluation method for 4G network based on attack tree model,which can be used to analyze the risks faced by the network and evaluate the risk level and security level of the system.The security risks of 4G network are categorized,and the attack tree model is constructed by sorting out the attack behavior and decomposing the attack flow.Then,the multi-attribute theory is used to give three security attributes to the leaf nodes and quantify them by scoring the level.The risk probability of the leaf node is calculated by combining Fuzzy Analytical Hierarchy Process(FAHP) and the fuzzy matrix.The risk probability of the root node is obtained according to the dependency between nodes.Experimental results show that the proposed method can accurately evaluate the risk factors of 4G network,predict the possible attack paths,and assist in the selection of security protection strategies.

【Key words】 4G network;security threats;attack tree model;risk assessment;Fuzzy Analytical Hierarchy Process(FAHP)
DOI: 10.19678/j.issn.1000-3428.0057483

0 概述

网络安全风险评估是利用一定的评估方法对系统的脆弱性以及面临的安全威胁进行综合分析,预测可能产生的后果并整体评价网络的安全风险,以便根据评估结果实施相应的安全策略,从而降低甚至消除风险。安全风险评估有利于了解系统的风险状况,发现潜在的安全缺陷,是制定防御策略并确保系统安全稳定的基础和前提。第四代移动通信技术(4G)自2010年发展至今,通信和传输速度更快,兼容性更好,应用也更广泛,截至2019年6月,4G用户数量达到12.3亿,占移动用户总数的77.6%,4G网络流量极速增加,成为移动互联网流量的主要来源。4G网络数据中涉及的用户隐私繁多,蕴含的价值丰富,是各种威胁行为的主要目标,一旦发生安全问题,造成的后果不仅是用户个人数据泄露,还可能对社会经济等产生影响。对4G网络进行安全风险评估,能够分析网络面临的风险因素和脆弱信息,了解风险所在,评估网络的安全性和防御性,该过程是选取恰当的防御手段以及部署有效防护策略的重要依据,也

基金项目: 国家自然科学基金青年基金项目(61803384)。
作者简介: 王赛娥(1990—),女,硕士研究生,主研方向为新一代通信网络、移动网络安全;刘彩霞,研究员、博士生导师;刘树新,助理研究员、博士;柏 溢,副研究员、硕士。
收稿日期: 2020-02-24 **修回日期:** 2020-04-07 **E-mail:** 951985329@qq.com

是确保4G网络安全的首要条件，具有一定的实际意义。

4G网络面临的安全威胁较多，既有传统的窃听、电信诈骗，还包含针对终端的恶意代码攻击、针对用户服务的DoS攻击等融合式威胁手段。现有的4G网络安全风险研究主要集中于探索系统未知的脆弱性和挖掘可利用的漏洞信息，主要分为协议分析法、模型检测法和经验分析法等。

协议分析法以协议本身作为风险研究核心，从协议标准、通信流程和协议内容等方面寻找不安全因素。协议分析可以利用安全协议验证工具辅助分析，文献[1]用形式化工具Tamarin分析5G AKA协议，将安全目标形式化，构建威胁模型，全面、系统地评估协议，分析结果确定了每个安全目标所需的最低安全假设并指出未满足的安全目标。文献[2]基于Lowe分类法对5G网络EAP-AKA′协议进行分析，发现了隐式鉴权方式下的安全问题和攻击路径。此外，可以使用数学逻辑对协议进行推理证明，常用的是BAN逻辑和类BAN逻辑。BAN逻辑是基于信仰的形式逻辑分析方法，后来发展出AUTLOG逻辑、SVO逻辑等类BAN逻辑。将要分析的协议改写成BAN逻辑或类BAN逻辑形式并作为既定条件，证明的假设前提是对协议双方的状态描述，结论是协议期望达到的安全目标，运用既定条件、假设前提和逻辑的推理规则进行证明，如果可以推导出结论则说明协议满足相应的安全目标。

模型检测法也称状态检测法，其运用有限状态机理论为系统建立模型，遍历状态空间，查找系统是否存在特殊状态或到达特殊状态的路径，由此检测系统是否违反了某些安全属性。文献[3]利用LTE Inspector检测4G LTE的附着、寻呼和去附着3个关键程序，发现了10个新的可用攻击和9个已知攻击，并在实验中验证了攻击的可行性和有效性。

经验分析法利用已知的攻击方法，逐一测试系统，根据攻击中系统的反馈不断调整攻击手段，通过攻击结果检验系统是否具有抵抗攻击的能力。该方法在原有伪基站攻击、协议攻击等的基础上进行改进，效率更高，但攻击结果可能会因为使用者的能力水平而稍有不同。

上述方法均以系统为中心，侧重于脆弱性研究从而挖掘可被利用的漏洞，但针对的安全威胁类型比较单一，缺少面对已知威胁的综合评估，没有涉及系统整体的安全风险状况。传统网络的安全风险评估发展已经成熟，有定性和定量的评估（如基于漏洞扫描和入侵检测的评估[4]）、基于知识推理的评估、基于资产价值的评估以及应用最广泛的基于模型的安全风险评估等。攻击树模型从攻击者角度出发，用图形化方式展现攻击流程，结合系统架构详细分析攻击方式并定量评估系统风险，其适合描述多阶段的复杂攻击行为，因此，在实际中得到广泛应用。文献[5]利用攻击树模型分析风电工业控制系统，对新能源行业控制系统进行评估，指导部署等级防护措施。4G通信网络架构清晰，面临的安全威胁多样，利用攻击树建模既能量化评估系统风险，又能显示攻击者最有可能的攻击路径，从而指出系统的薄弱处以便管理人员重点防控。

本文提出一种基于攻击树的4G网络安全风险评估方法，改进攻击树模型以适配4G网络架构，运用多属性理论和模糊层次分析法（Fuzzy Analytical Hierarchy Process，FAHP）评估4G网络面临已知安全威胁时的风险等级，对系统脆弱性及可能产生的后果进行预测和定量分析，根据评估结果提出有效的防护措施，从而降低网络安全风险。

1 研究背景

1.1 4G网络架构

相比传统的2G、3G网络，4G网络架构有较大改变，其分为接入网E-UTRAN（Evolved Universal Terrestrial Radio Access Network）和核心网EPC（Evolved Packet Core）2个部分，如图1所示。

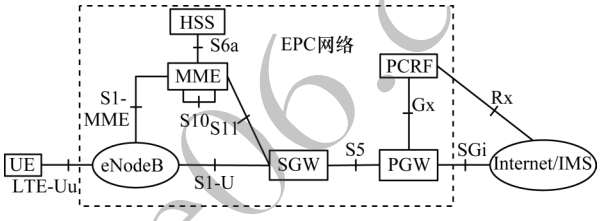

图1 4G网络架构

Fig.1 4G network architecture

在E-UTRAN中，采用更扁平化的网络结构，网元种类减少，取消3G中的无线网络控制器（Radio Network Controller，RNC），只包含基站eNodeB（Evolved Node B）。eNodeB是无线接入网网元，负责空中接口相关的功能，部分RNC功能也集成到了eNodeB中，主要包括物理层功能、无线资源管理、无线接入控制、承载控制和移动管理等。eNodeB直接接入EPC中，能够降低通信时延，提高通信速率。

核心网EPC主要包括移动管理实体（MME）、服务网关（SGW）、分组数据网关（PGW）、归属签约数据库（HSS）以及策略控制和计费规则单元（PCRF）。

MME是接入网络的关键点，主要负责用户接入控制、安全控制、信令处理、移动性管理等。SGW是用户面接入服务网关，负责用户面数据处理，在MME的控制下进行数据包路由和转发、传输层上下行数据标记以及下行数据包缓存等。PGW也是用户面的网元，是EPC的边界网关，主要完成会话和承载管理以及IP地址分配的功能。HSS是存储用户签约信息的数据库，其存储用户数据、位置信息和标识信息等，同时也是网络的鉴权中心，执行身份验证和授权操作。PCRF负责策略控制和计费，其提供可用的策略和控制决策，主要进行规则制定，不具备具体

计费功能，可根据用户提供的信息进行决策，确定业务和计费策略。

在EPC网络中，取消电路域CS（Circuit Switched），采用单一网络架构，各网元间使用IP传输，实现全网IP化，同时控制与承载分离，信令面功能由MME负责，用户面功能由SGW承担。

LTE在安全方面采取分层机制，将接入层和非接入层分离，两层有各自的密钥和机制。接入层确保用户和基站之间的安全，非接入层确保用户和MME之间的安全。分层设计使得两层之间相互影响较小，从而提高了系统整体的安全性。

1.2　4G网络典型安全威胁

尽管4G网络架构考虑了安全性问题，但是在实际中仍面临很多安全威胁，根据威胁利用的主要位置可以分为用户设备威胁、接入网威胁和核心网威胁，它们的目的是窃取用户隐私数据、造成用户服务中断等。

造成用户信息泄露的威胁具体如下：

1）窃听，又称流量分析，其可以利用无线信道的开放性，通过空口协议存在的漏洞直接获取所传输的信息，如果不能直接解码消息内容，可以依据消息的源地址和目的地址，通过消息流来推断内容。

2）伪基站攻击[6]，其通过设立恶意基站增强信号强度，使目标用户主动附着，用户所有数据均经过伪基站中转，从而获取和篡改其中所传输的信息。伪基站攻击可以实现多种攻击效果，获取合法用户身份信息、窃取目标用户位置信息以及中断用户合法服务请求等。在实际中，伪基站攻击因为攻击成本低、简便易操作等原因，成为很多攻击者首选的威胁手段。

3）恶意代码威胁[7]，其与传统互联网领域的攻击方式极为相似，利用用户设备端操作系统或者应用软件的漏洞控制用户设备，搜集用户数据，获取用户权限等。该威胁在移动通信网中通常与伪基站相结合，在用户设备接入伪基站后向用户发送伪造的虚假短信、钓鱼链接等，诱骗用户点击触发恶意代码，从而窃取用户信息。

4）位置追踪攻击。文献[8]发现运营商实际部署中GUTI重分配规则存在固定字节以及重分配规律可预测的漏洞。攻击者对用户进行多次静默呼叫，触发寻消息，监听并记录消息中的GUTI值，根据重分配规则来推测用户是否在该区域。

致使用户服务中断或者扰乱用户正常通信的常见威胁具体如下：

1）假冒攻击[9]，指攻击者获知目标用户手机号或其他身份信息后，假冒用户身份在网络中注册，以目标用户身份合法使用网络服务，造成受害者不能正常接入网络。

2）基站资源消耗攻击[10]。攻击者利用基站有最大活动用户连接量的特性，使用恶意软件等技术手段假冒不同身份的用户发起连接请求，消耗基站资源，达到最大连接量后基站拒绝所有合法用户的连接请求。

3）Blind DoS攻击[10]，该攻击方式和假冒攻击有相似之处，与基站通信时都需要假冒目标用户的身份，不同的是，该攻击更具针对性，能够有选择地中断目标用户的特定服务，其可以假冒用户特定服务的通信流程，只针对特定服务进行干扰，隐蔽性更强，不易察觉。

4）同步验证失败攻击[3]，其利用用户与基站通信过程中的序列号（SQN）一致性检查，攻击者假冒用户身份，在连续的连接请求中采用不同的安全选项（选择不同的加密或完整性保护算法），使HSS认为是多个不同请求，处理时增加自身的SQN值，造成用户端和HSS端的SQN值不同步。当用户端对SQN检查时，如果超出规定范围，则校验与连接建立均失败。

5）信令协议攻击，其利用通信流程中信令协议的脆弱性，拦截正常的通信消息，修改消息内容进行通信扰乱，如利用4G核心网中的DIAMETER信令干扰通信。

4G网络面临的安全威胁还有很多，其具体攻击方法与传统互联网攻击有所不同，但攻击效果类似，其中部分攻击方法从互联网攻击手段中发展而来。互联网对类似的安全威胁进行评估，大多需要借助专业工具，结合不同工具的评估结果给出系统整体的安全风险值。基于系统漏洞的评估使用漏洞扫描工具，根据通用漏洞评估方法（CVSS）等评价标准给出系统漏洞的危险等级，从而评估系统风险。基于入侵检测的评估方式分析攻击行为的特征并设立知识库，通过研究网络中数据与知识库的匹配度来评估网络安全风险。此类方法都是从系统层面出发，以工具为基础，依赖相应的知识库或漏洞库，缺少全面的评估标准，而且不能完整地分析攻击流程，评估结果依赖于知识库的完善度和及时更新。本文提出的基于攻击树的评估方法，从攻击层面出发，包含完整的攻击流程分析且具有一定的通用性，在风险评估的同时还可以分析攻击场景，从而使防御更有针对性。

2　基于攻击树的安全风险评估

基于攻击树模型的安全风险评估主要分为2个阶段：第一阶段分析系统面临的安全威胁，根据节点关系构建层次化的攻击树模型；第二阶段计算风险，根据威胁行为特点赋予叶节点相应的属性并进行量化，从而计算根节点的风险概率。

2.1　攻击树模型

攻击树是对目标基础设施可能遭受的攻击的层次化描述，其从故障树[11]演变而来，被SCHNEIER[12]广泛推广。SCHNEIER将攻击树作为一种安全威胁的建模方法，利用层次化进行表示，通过自下而上的单参数扩散来进行定量的安全评估。攻击树模型[13]

构建简单,易于理解,图形化方式较为直观,适合描述详细的攻击过程并评估系统面临的安全风险。

树的根节点表示攻击的最终目标,子节点表示实现该目标的子目标,层层细化,最后的叶节点表示不可分解的原子攻击,从根节点到叶节点的路径表示实现目标的一个完整攻击流程,攻击树表示实现目标的所有可能的攻击路径。节点之间的基本关系有“与”“或”两种,“与”表示节点代表的手段和方法要同时完成才可以实现父节点,“或”表示只要完成一个子节点就可以实现父节点。

在实际应用中,子目标或者行为之间通常存在严格的顺序约束关系,打乱顺序则不能实现特定目标,而攻击树的“与”“或”关系不能被准确描述,因此引入扩展节点,其依赖关系为“顺序与”,即节点必须按照顺序关系依次完成才能实现父节点目标。扩展后的攻击树节点表示如图2所示,扩展攻击树模型能够准确描述子攻击行为之间的相关性,构建完成后对节点的属性(攻击成本、攻击难度等)赋值,计算子节点的风险值,然后根据节点之间的依赖关系得到目标的风险值。

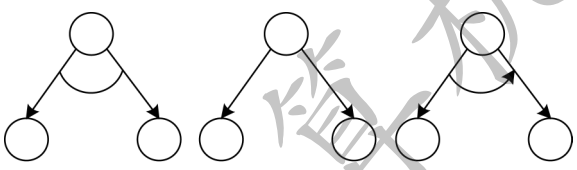

图2 攻击树的节点表示方法

Fig.2 Node representation methods of attack tree

2.2 4G网络的扩展攻击树模型构建

攻击树可以看作具有根节点的图,能够通过向后推理的过程来构建。首先,确定一个目标作为根节点,本文将4G网络面临的安全威胁作为目标;然后,分析能够造成威胁的前提或事件的组合,将其作为子节点,通过“与”“或”“顺序与”的关系表示,将子节点层层拆分,直到成为不可拆分的原子攻击,将其作为叶节点。从根节点到叶节点的一条路径是一个攻击序列,代表一次完整的攻击流程。

攻击树模型在面向复杂的大型网络时,建模效率较低,且随着系统规模的增加,分支数呈指数级增长,可能带来空间爆炸的问题,攻击路径的搜索难度大幅提升,因此,攻击树不具有通用性。现有研究多数是针对简单网络或单一安全威胁,文献[14]使用攻击树对车载自组织网络的位置隐私泄露风险进行建模,文献[15]将攻击树模型用于木马检测,但针对的是恶意代码攻击这种单一威胁手段。文本提出的4G网络扩展攻击树模型,针对多种安全风险,具备数据重用性,同时,为降低树的复杂度,本文在构建扩展攻击树的过程中,引入STRIDE[16]威胁分类模型,其可以限制一级节点数量,从而有效减少分支数并压缩树的宽度。

STRIDE模型将常见的安全威胁分成身份欺骗、数据篡改、抵赖、信息泄露、拒绝服务和权限提升6个维度,可以涵盖目前绝大部分的安全威胁,同时,这6个维度与信息安全属性相关。信息安全的3个基本属性[17]是机密性、完整性和可用性,除此之外还包括可靠性、不可抵赖性和可控性等其他属性。STRIDE模型与信息安全属性的对应关系如表1所示。

表1 STRIDE模型及安全属性

Table 1 STRIDE model and security attributes

安全威胁	定义	对应的安全属性
身份欺骗	假冒他人身份	鉴权
数据篡改	修改数据	完整性
抵赖	否认某个操作	不可抵赖性
信息泄露	机密消息泄露	机密性
拒绝服务	不提供服务	可用性
权限提升	未经授权获得许可或超出授权范围	授权

STRIDE模型的6个维度将安全威胁进一步细化,因此,STRIDE模型可以作为第一级节点。结合典型的攻击方式,将4G网络可能面临的安全威胁整理成攻击树,如图3所示。

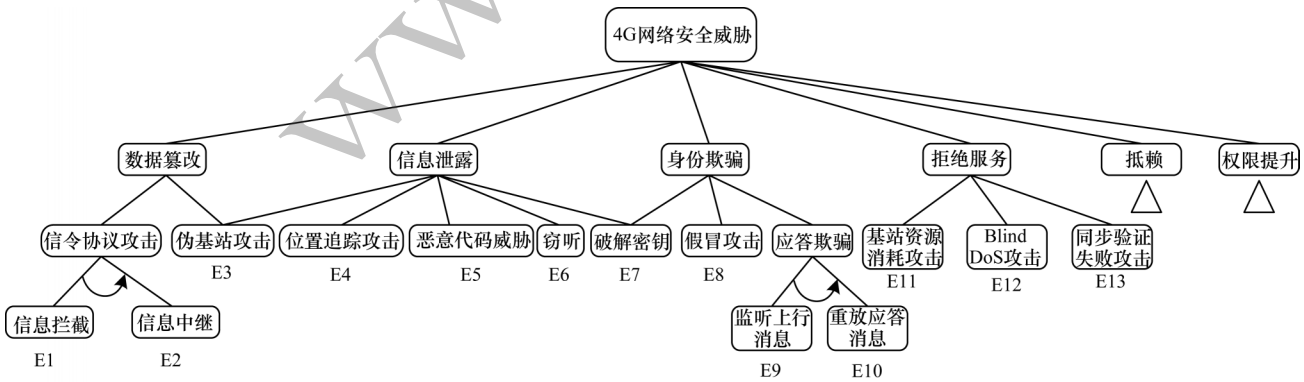

图3 4G网络攻击树

Fig.3 Attack tree of 4G network

在攻击树中，第一级节点为STRIDE模型，本文攻击树暂不涉及权限提升和抵赖2种安全威胁。能够到达根节点的路径（即对4G网络造成安全威胁的事件组合）称为攻击序列，如S1{E1，E2}。一个攻击树中存在多个攻击序列，它们都对根节点造成安全威胁。

2.3　风险评估算法研究

2.3.1　叶节点风险概率

本文对攻击树模型的评估采用属性的观点，根据4G网络攻击行为特点，赋予每个叶节点3个属性：实现攻击的花销cost，技术难度dif，发现难度det。运用多属性效用论[18-20]可以计算得到叶节点的风险概率，具体如下：

$$P_a = W_{\text{cost}} \times U\left(\text{cost}_a\right) + W_{\text{dif}} \times U\left(\text{dif}_a\right) + W_{\text{det}} \times U\left(\text{det}_a\right) \tag{1}$$

其中，a表示一个任意的叶节点，P_a表示叶节点的风险概率，cost_a、dif_a、det_a分别表示节点a的攻击花销、技术难度和发现难度，U表示对应属性的效用值，W表示对应参数的权重，3个权重之和为1。

叶节点的3个属性可以采用等级评分的方法量化，评分标准如表2所示。将3个属性划分为5个等级，依据评估标准对叶节点的属性进行评级。

表2　安全属性等级评分标准

Table 2　Safety attributes rating standard

等级	攻击花销/千元	技术难度	发现难度
5	>10	困难	困难
4	5~10	较困难	较困难
3	2~5	中等	中等
2	1~2	较容易	较容易
1	<1	容易	容易

攻击花销以购买设备或软件等花费为参考，技术难度以攻击实施的复杂性为参考，发现难度以漏洞等级为参考。在实际应用中，可以采取专家打分的方式赋值，也可以借鉴通用的漏洞库和漏洞评分系统，如CVE、CVSS等。

分析可知，属性的等级与其效用值成反比，因此，$U(x)=c/x$，其中，c为常数，为了方便后续计算，通常取c值为1，即$U(x)=1/x$，由此可以得到各节点属性的效用值。各属性的权重有不同的计算方法，文献[20]使用数学归纳法，根据实际情况推导出权重；文献[21]使用层次分析法，将权重按照属性分解成多个层次，从而较好地衡量指标的相对重要性。但是，上述2种方法主观性较强，结果差异性较大。本文采用模糊层次分析法（FAHP）[22-24]对指标进行比较和模糊性处理[25]，从而降低主观因素对评估结果的影响。首先，根据叶节点所在层级被攻击后各元素对上一层的影响确定其相对重要性，然后，将重要性进行两两比较，建立模糊判断矩阵。建立矩阵时的比较尺度表选用0.1~0.9标度，如表3所示。

表3　比较尺度表

Table 3　Comparison scales table

尺度	含义
0.9	一个元素比另一个元素十分重要
0.8	一个元素比另一个元素重要很多
0.7	一个元素比另一个元素重要
0.6	一个元素比另一个元素稍微重要
0.5	2个元素重要程度相等
0.1~0.4	反比较，若元素a_i与a_j比较得到r_{ij}，则a_j与a_i比较得到$r_{ji}=1-r_{ij}$

根据上述尺度表，可以得到模糊判断矩阵如下：

$$\boldsymbol{R}=\begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nn} \end{bmatrix}$$

根据模糊一致矩阵[26]的定义，$\forall k$有$r_{ij}=r_{ik}-r_{jk}+0.5$，对矩阵$\boldsymbol{R}$进行一致性检验[27]，如果矩阵不满足一致性，则要根据：

$$r'_{ij}=\frac{1}{2n}\sum_{k=1}^{n}(r_{ik}-r_{jk})+0.5 \tag{2}$$

将$\boldsymbol{R}$转变为模糊一致矩阵$\boldsymbol{R}'$，归一化处理后，得到各属性的权重W_i：

$$W_i=\frac{1}{n}-\frac{1}{2a}+\frac{1}{na}\sum_{k=1}^{n}r'_{ik} \tag{3}$$

其中，n是构造的矩阵阶数，a为权重影响因子，其与权重的差异成反比，即a越大，差异越小，且$a\geqslant(n-1)/2$。在计算中，取$a=(n-1)/2$，即取权重差异最大的情况，将求得的W_i和U_i代入式（1）即可得到叶节点的风险概率P_a。

2.3.2　根节点风险概率

根节点的实现是攻击序列完整执行的结果，因此，计算根节点首先需要整理出所有的攻击序列，计算出序列中所有叶节点的风险概率，然后再依据节点之间的依赖关系计算父节点概率，自下而上分层计算，最终得到根节点的风险概率。父节点的风险概率计算与子节点的“与”“或”和“顺序与”3种依赖关系有关：

1）在“与”关系中，父节点风险概率等于各子节点风险概率之积：

$$P=P_1\times P_2\times\cdots\times P_n \tag{4}$$

2）在“或”关系中，父节点风险概率取各子节点风险概率中的最大值：

$$P=\max\{P_1,P_2,\cdots,P_n\} \tag{5}$$

3）在“顺序与”关系中，父节点风险概率符合条件概率的情况：

$$P=P_{n_1}\times P_{(n_2|n_1)}\times\cdots\times P_{(n_n|n_1n_2\ldots n_{n-1})} \tag{6}$$

由此，自下而上可以逐级推断出每层节点的风险概率，最终得到根节点风险概率，即4G网络的安全风险评估结果，在过程中也可以得到单一安全威胁事件的风险概率，即对应的攻击序列的发生概率。

3 实验结果与分析

3.1 环境介绍

为避免影响真实用户,本文在实验室搭建的4G网络环境下进行测试,所有设备均来自中兴公司,网络拓扑如图4所示。模拟用户号段CS:1619800XXXX,VoLTE:1619900XXXX。

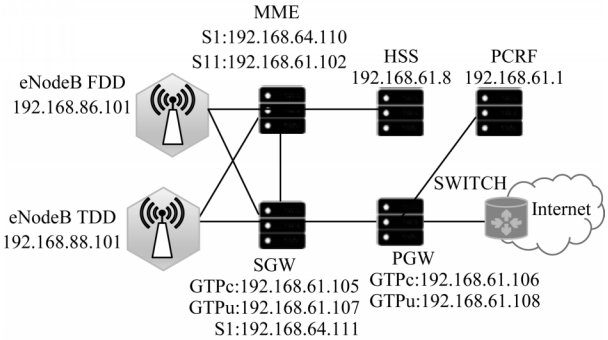

图4 4G网络拓扑

Fig.4 4G network topology

3.2 威胁分析

在实验中模拟攻击方时,硬件采用USRP B210,软件使用爱尔兰SRS(Software Radio Systems)公司开发的免费开源LTE框架srsLTE,支持srsUE和eNodeB,可以模拟恶意UE或LTE网络。本文以STRIDE模型中拒绝服务为攻击目标,即以模拟用户服务被拒绝或网络不能正常提供服务为攻击目标,构建攻击树模型,如图5所示。图5中各节点符号的具体含义如表4所示。按照攻击可能发生的位置将威胁分为3种:针对终端发起的攻击,针对网元发起的攻击,针对通信流程发起的攻击,它们是第一级节点。在实验中,终端用的是智能手机,因此,第一种威胁主要是针对智能手机的恶意代码攻击,又可以细分为用户被动触发和攻击者主动控制两类。针对网元发起的攻击包括基站受到的威胁、核心网作为整体受到的威胁和物理层面遭到的破坏。针对通信流程发起的攻击主要利用信令协议,更改协议中消息内容或延迟响应等,破坏正常的通信进程,扰乱会话从而造成安全威胁。

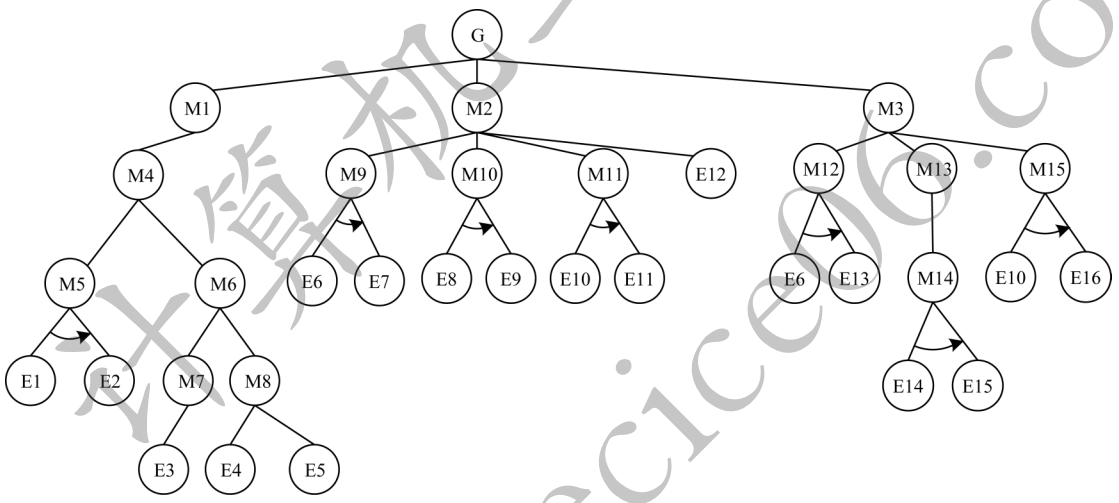

图5 实验室环境下4G网络拒绝服务攻击树

Fig.5 4G network denial of service attack tree in laboratory environment

表4 攻击树中各节点的符号含义

Table 4 Symbolic meaning of each node in attack tree

符号	含义	符号	含义
G	拒绝服务	E1	编写含有恶意代码的消息、应用、网页等
M1	针对终端发起攻击	E2	伪装后推送给用户或伪装成合法应用进行发布
M2	针对网元发起攻击	E3	远程代码执行漏洞
M3	针对通信流程发起攻击	E4	机主授权
M4	恶意代码	E5	获取终端密码
M5	诱使用户点击或下载	E6	搭建伪基站
M6	攻击者主动写入	E7	目标用户接入
M7	远程控制	E8	软件模拟多用户
M8	物理控制	E9	频繁重启随机访问
M9	伪基站攻击	E10	获取目标用户S-TMSI
M10	基站资源消耗攻击	E11	伪装成目标用户向MME发送消息
M11	远程注销攻击	E12	物理破坏
M12	寻呼通道劫持	E13	在目标用户的寻呼周期广播假消息
M13	身份验证同步失败攻击	E14	获取目标用户IMSI
M14	序列号SQN不同步	E15	伪装成用户向HSS发送不同的附着消息
M15	Blind DoS攻击	E16	伪装成目标用户发起RRC连接

在生成的攻击树模型中，共包含11组可以造成拒绝服务的攻击序列Si，分别为S1{E1，E2}、S2{E3}、S3{E4}、S4{E5}、S5{E6，E7}、S6{E8，E9}、S7{E10，E11}、S8{E12}、S9{E6，E13}、S10{E14，E15}和S11{E10，E16}。执行任一攻击序列都能使模拟用户服务失常，多节点的序列中节点之间的依赖关系是“顺序与”，其先后不能被打乱，否则无法正确执行。

3.3　评估结果与对比

对生成的攻击树模型按照安全风险评估算法进行评估，利用表2的评估标准对各节点的攻击花销、技术难度和发现难度属性进行打分[28]，具体如表5所示。

表5　叶节点的安全属性等级得分

Table 5　The security attributes rating scores of leaf nodes

叶节点	攻击花销	技术难度	发现难度
E1	1	2	1
E2	4	2	2
E3	3	5	5
E4	1	4	4
E5	2	4	4
E6	5	2	1
E7	1	1	1
E8	5	2	1
E9	1	1	1
E10	3	3	2
E11	2	2	1
E12	4	5	5
E13	1	3	3
E14	3	4	4
E15	2	2	3
E16	2	2	1

根据相对重要性，将各属性的权重值进行两两比较得到模糊判断矩阵：

$$\boldsymbol{R}=\begin{bmatrix}0.5 & 0.2 & 0.1\\ 0.8 & 0.5 & 0.3\\ 0.9 & 0.7 & 0.5\end{bmatrix}$$

对矩阵进行一致性检验，发现不具有一致性，根据式(2)将其转换为模糊一致矩阵，随后用式(3)进行归一化处理，因为要赋予叶节点3个安全属性，所以式(3)中n取值为3，a取值为1，计算可得权重W_{cost}值为0.22，W_{dif}值为0.35，W_{det}值为0.43。最后，根据节点间的依赖关系，得出11组攻击序列的风险概率如表6所示。为了验证评估方法的有效性，对已生成的攻击树模型采用文献[29]方法进行评估，结果如表7所示。

表6　攻击序列的风险概率

Table 6　Risk probability of attack sequences

攻击序列	风险概率	攻击序列	风险概率
S1	0.37	S7	0.29
S2	0.23	S8	0.21
S3	0.42	S9	0.31
S4	0.31	S10	0.11
S5	0.65	S11	0.29
S6	0.65		

表7　文献[29]方法评估结果

Table 7　Evaluation results of the method in literature[29]

攻击序列	发生概率	攻击序列	发生概率
S1	0.39	S7	0.32
S2	0.21	S8	0.20
S3	0.33	S9	0.30
S4	0.28	S10	0.10
S5	0.74	S11	0.32
S6	0.74		

从图6可以看出，2种方法攻击序列的风险概率有一定差异，主要原因是两者的属性权值计算方法不同。文献[29]方法使用算术平均法对矩阵进行处理，最终W_{cost}值为0.1，W_{dif}值为0.37，W_{det}值为0.53，攻击序列S5、S6的可能性仍旧最高，但实际中这2种攻击方式也是最容易被察觉的，因此，发生概率较低。本文方法所得结果更贴合实际情况，同时文献[29]方法中攻击花销的权重值极小，降低了攻击花销属性对攻击方式选择结果的影响，可信度不高。

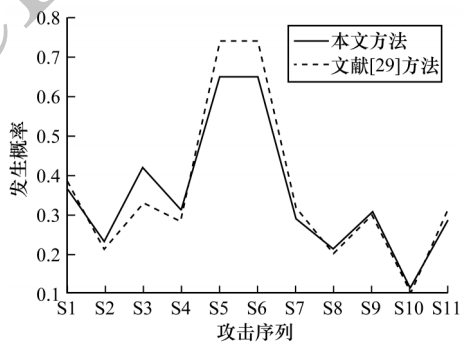

图6　本文方法与文献[29]方法评估结果对比

Fig.6　Comparison of the evaluation results between the method in this paper and the method in literature[29]

综上，本文方法所得概率较为平稳，能够清晰反映最有威胁性的攻击行为，具备较高的可信度，构造的攻击树模型也有一定的通用性，能真实反映4G网络的风险状况，根据评估结果部署防御措施能够在有限的范围内选择最有利的防御行为，大幅提高系统的安全性。由评估结果可知，实验室环境中网络最有可能受到的安全威胁是由攻击序列S5和S6造

成的,即伪基站攻击和基站资源消耗攻击。在实际情况中,伪基站攻击和基站资源消耗攻击也是移动通信网面临的最常见、最通用的威胁手段。

目前,运营商和公安系统联手加大了对各种攻击手段的打击力度,但是仍有部分不法分子不断升级攻击技术和隐蔽性,这类攻击可以造成用户在较短时间内与正常的运营商网络断开连接,然后结合恶意代码对用户造成威胁。评估结果中恶意代码系列的攻击概率较高,这需要用户增强防范意识,切勿随意点击不明来源的链接,不轻易扫描不明二维码,仔细辨别信息内容,防止泄露个人信息。智能终端上也可以使用安全软件,监控系统的敏感数据,及时发现危险操作,阻止恶意代码入侵。

4 结束语

安全风险评估是保障系统安全稳定的基础,只有全面、系统地掌握网络状态及其面临的安全风险,才能更好地实施防御策略。本文在梳理4G网络安全威胁的基础上,提出4G网络攻击树构造方法,使用扩展节点融合STIDE模型,以真实反映系统情况并限制攻击树的规模,然后通过模糊层次分析法进行安全风险评估。实验结果验证了该方法的有效性。对4G网络建模、构造攻击树以及量化评估风险发生概率,有利于分析网络的安全状况和攻击者可能采取的攻击路径,从而有针对性地进行防御,提高系统安全等级。但在面对大规模网络时人工建模效率低、耗费时间长,因此,下一步将减少人为因素的干扰并实现一种自动化风险评估方式,以提高评估结果的客观性、准确性以及通用性。

参考文献

[1] BASIN D,DREIER J,HIRSCHI L,et al. A formal analysis of 5G authentication[C]//Proceedings of 2018 ACM SIGSAC Conference on Computer and Communications Security. New York,USA:ACM Press,2018:16-23.

[2] LIU Caixia, HU Xinxin, LIU Shuxin, et al. Security analysis of 5G network EAP-AKA′ protocol based on lowe classification[J]. Journal of Electronics and Information Technology,2019,41(8):1800-1807. (in Chinese)
刘彩霞,胡鑫鑫,刘树新,等. 基于Lowe分类法的5G网络EAP-AKA′协议安全性分析[J]. 电子与信息学报,2019,41(8):1800-1807.

[3] HUSSAIN S R,CHOWDHURY O,MEHNAZ S,et al. LTEInspector:a systematic approach for adversarial testing of 4G LTE[C]//Proceedings of 2018 Network and Distributed System Security Symposium. Washington D. C. ,USA:IEEE Press,2018:156-169.

[4] HOLM H, SOMMESTAD T, ALMROTH J, et al. A quantitative evaluation of vulnerability scanning[J]. Information Management & Computer Security, 2011, 19(4):231-247.

[5] CHEN Qixiang. Information security risk assessment method for control system of wind power plant[J]. Electronics World,2020(1):42-43,46. (in Chinese)
陈其祥. 一种风电厂控制系统信息安全风险评估方法[J]. 电子世界,2020(1):42-43,46.

[6] ZHANG Wanqiao,YANG Qing. LTE redirection:forcing targeted LTE cellphone into unsafe network[EB/OL]. [2019-12-25]. https://ruxcon. org. au/assets/2016/slides/LTE_Redirection_Ruxcon. pdf.

[7] MJØLSNES S F, OLIMID R F. Easy 4G/LTE IMSI catchers for non-programmers[M]. Berlin, Germany: Springer,2017.

[8] HONG B,BAE S,KIM Y. GUTI reallocation demystified:cellular location tracking with changing temporary identifier[C]//Proceedings of 2018 Network and Distributed System Security Symposium. Washington D. C. ,USA:IEEE Press,2018:25-36.

[9] RUPPRECHT D,KOHLS K,HOLZ T,et al. Breaking LTE on layer two[C]//Proceedings of 2019 IEEE Symposium on Security and Privacy. Washington D. C. ,USA:IEEE Press,2019:123-156.

[10] KIM H,LEE J,LEE E,et al. Touching the untouchables:dynamic security analysis of the LTE control plane[C]//Proceedings of 2019 IEEE Symposium on Security and Privacy. Washington D. C. ,USA:IEEE Press,2019:1153-1168.

[11] VESELY W E,GOLDBERG F F,ROBERTS N H,et al. Fault tree handbook[EB/OL]. [2019-12-25]. https://www. nrc. gov/docs/ML1007/ML100780465. pdf.

[12] SCHNEIER B. Attack trees[J]. Doctor Dobbs Journal, 1999,24(12):21-29.

[13] LIU Wenyan,HUO Shumin,TONG Qing,et al. Research on network security evaluation and analysis model[J]. Chinese Journal of Network and Information Security, 2018,4(4):1-11. (in Chinese)
刘文彦,霍树民,仝青,等. 网络安全评估与分析模型研究[J]. 网络与信息安全学报,2018,4(4):1-11.

[14] DU S G,ZHU H J. Security assessment via attack tree model[M]//DU Suguo, ZHU Haojin. Security assessment in vehicular networks. Berlin,Germany:Springer, 2013:9-16.

[15] CHEN Yanhong, OU Yuyi , LING Jie. An improved trojan horse detection method based on extended attack tree model[J]. Computer Applications and Software, 2016,33(8):308-311. (in Chinese)
陈燕红,欧毓毅,凌捷. 一种改进的基于扩展攻击树模型的木马检测方法[J]. 计算机应用与软件,2016,33(8):308-311.

[16] HERNAN S,LAMBERT S,OSTWALD T,et al. Uncover security design flaws using the STRIDE approach(2006)[EB/OL]. [2019-12-25]. http://msdn. microsoft. com/en-gb/magazine/cc163519.

[17] FAN Hong. Understanding and implementation of national standards for information security risk assessment[M]. Beijing: China Standard Press, 2008. (in Chinese)
范红. 信息安全风险评估规范国家标准理解与实施[M]. 北京:中国标准出版社,2008.

[18] BULDAS A, LAUD P, PRIISALU J, et al. Rational choice of security measures via multi-parameter attack trees[M]. Berlin,Germany:Springer,2006.

(下转第154页)

（上接第146页）

[19] MATEO J R S C. Multi-attribute utility theory[M]. Berlin, Germany: Springer, 2012.

[20] GAN Zaobin, WU Ping, LU Songfeng, et al. Risk assessment of information system security based on extended attack tree[J]. Application Research of Computers, 2007, 24(11): 153-156. (in Chinese)
甘早斌,吴平,路松峰,等. 基于扩展攻击树的信息系统安全风险评估[J]. 计算机应用研究,2007,24(11):153-156.

[21] HE Mingliang, CHEN Zemao, LONG Xiaodong. Improvement of attack tree model based on analytic hierarchy process[J]. Application Research of Computers, 2016, 33(12): 3755-3758. (in Chinese)
何明亮,陈泽茂,龙小东. 一种基于层次分析法的攻击树模型改进[J]. 计算机应用研究,2016,33(12):3755-3758.

[22] CHAN H K, WANG X J. Fuzzy hierarchical model for risk assessment[M]. Berlin, Germany: Springer, 2013.

[23] FU Y, WU X P, YE Q. Approach for information systems security situation evaluation using improved FAHP and Bayesian network[J]. Journal on Communications, 2009, 30(9): 135-140.

[24] TAYLAN O, BAFAIL A O, ABDULAAL R M S, et al. Construction projects selection and risk assessment by fuzzy AHP and fuzzy TOPSIS methodologies[J]. Applied Soft Computing, 2014, 17: 105-116.

[25] ZHANG Jijun. Fuzzy Analytic Hierarchy Process(FAHP)[J]. Fuzzy Systems and Mathematics, 2000, 14(2): 80-88. (in Chinese)
张吉军. 模糊层次分析法(FAHP)[J]. 模糊系统与数学,2000,14(2):80-88.

[26] TAO Yuhui. How to construct fuzzy consistent judgment matrix in fuzzy analytic hierarchy process[J]. Journal of Sichuan Normal University(Natural Science), 2002, 23(3): 282-285. (in Chinese)
陶余会. 如何构造模糊层次分析法中模糊一致判断矩阵[J]. 四川师范学院学报(自然科学版),2002,23(3):282-285.

[27] SONG Guangxing, YANG Deli. Consistency check and improvement method of fuzzy judgment matrix [J]. Systems Engineering, 2003, 21(1): 110-116. (in Chinese)
宋光兴,杨德礼. 模糊判断矩阵的一致性检验及一致性改进方法[J]. 系统工程,2003,21(1):110-116.

[28] GEER D, HOO K S, JAQUITH A. Information security: why the future belongs to the quants[J]. IEEE Security & Privacy, 2003, 1(4): 24-32.

[29] LÜ Zongping, QI Wei, GU Zhaojun. Attack tree model based on fuzzy analytic hierarchy proces[J]. Computer Engineering and Design, 2018, 39(6): 1501-1505, 1515. (in Chinese)
吕宗平,戚威,顾兆军. 基于模糊层次分析法的攻击树模型[J]. 计算机工程与设计,2018,39(6):1501-1505,1515.

编辑　吴云芳