计算机免疫危险理论中危险信号的提取方法研究

杨 超[1] 李 涛[2]

(湖北大学计算机与信息工程学院 武汉 430062)[1] (武汉科技大学计算机科学与技术学院 武汉 430065)[2]

摘 要 危险理论是人工免疫系统的一个重要研究分支,它从危险的角度出发对免疫系统的工作原理进行了新的阐述,目前已广泛应用于入侵检测、机器学习和数据挖掘等领域。建立危险理论模型的首要问题是如何自适应地提取危险信号。从变化导致危险这一思想出发,建立了一套基于变化特征的危险信号自适应提取模型;针对不同类型系统资源的特点,设计了基于值变化和特征变化的两种危险信号提取方法。同时,通过实验验证了该模型在不依赖先验知识的情况下,能够自适应地提取危险信号。

关键词 人工免疫系统,危险理论,危险信号,变化提取

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.8.036

Research of Danger Signal Extraction Based on Changes in Danger Theory

YANG Chao[1] LI Tao[2]

(School of Computer Science and Information Engineering, Hubei University, Wuhan 430062, China)[1]

(College of Computer Science and Technology, Wuhan University of Science and Technology, Wuhan 430065, China)[2]

Abstract Danger theory is an important research branch in artificial immune system. It starts from the perspective of danger to describe the working principle of immune system in a new way, which has been widely used in intrusion detection, machine learning, data mining and so on. The primary issue of establishing a danger theory model is how to extract danger signals adaptively. This paper started from the main idea of changes leading to danger, and established an adaptive danger signal extraction model based on finding changes. According to the characteristics of different types of system resources, it designed two danger signal extraction methods: value changes and feature changes. The experiment verifies that this model can adaptively extract danger signals without relying on prior knowledge.

Keywords Artificial immune system, Danger theory, Danger signal, Change extraction

1 引言

2002年,英国诺丁汉大学的Uwe研究小组在文献[1]中提出并在理论上证明了以反向选择模型为基础的人工免疫系统中存在的可计算问题和伪肯定率较高等问题,首次提出了可以将机体免疫系统中的危险理论引入计算机安全领域来解决上述问题,并对危险理论可能的应用领域做出了假设。十多年来,危险理论作为人工免疫学中一种新兴的理论方法,已经广泛应用于入侵检测[2,3]、机器学习[4]、数据挖掘[5]等研究领域,并取得了较好的研究成果。

危险理论研究和应用的重点在于定义何为危险,即危险信号的定义问题。危险信号是危险理论的基础,是激活抗原提呈细胞,启动免疫应答的关键。同时,危险信号也是诱发危险的潜在因素,危险信号的定义直接影响着检测系统能否正确、有效地捕捉到系统中的危险。

然而,目前以DCA算法为代表的危险理论研究中,危险信号的定义存在智能性[6]和完备性缺乏的问题[7],即危险信号的定义依赖人工经验,缺乏智能性。同时由于危险信号的定义依赖人工经验,难以覆盖全部的危险特征,导致以此为基础的检测系统难以有效捕捉到危险,从而影响了检测的效率。

危险的发生,通常表现为系统功能受到损害,各种维持系统稳定的平衡状态遭到破坏。这些破坏往往是由大量微小变化共同积累、相互作用带来的,即通常所说的"量变导致质变"。因此,这些微小变化正是导致系统从正常向异常过渡的关键因素,也是我们所关注的危险产生的诱因,即危险信号。无论是由于外部入侵所产生的抗原相关分子模式(Pathogen-associated Molecular Pattern,PAMP)信号还是系统内部病变所产生的危险报警信号(Alarmins),都会带来系统异常的变化[8],这些变化就是危险产生的前奏或危险造成的结果。本文尝试通过分析这些变化中的正常和异常来感知危险,实现危险信号的普适性定义和一般性描述。

2 相关工作

2.1 危险信号的人工定义问题

DCA算法是危险理论的典型应用之一,在该算法中定义了PAMPs信号、安全信号和危险信号,通过这3种信号的共

到稿日期:2014-09-29 返修日期:2014-10-12 本文受国家自然科学基金项目(61170306),湖北省自然科学基金面上项目(2014CFB536),湖北省教育厅人文社科重点项目(2012D111)资助。

杨 超(1982-),男,博士,讲师,主要研究方向为信息安全、人工免疫学,E-mail:stevenyc@hubu.edu.cn;李 涛(1979-),男,博士,副教授,主要研究方向为信息安全、智能计算。

同作用来确定系统中是否有危险存在。在其应用过程中，无论是进行 SYN[9]和 Ping 扫描检测[10]，还是对僵尸网络(Botnet)进行检测，或者应用于数据挖掘领域[11]，对 3 种信号的定义都依赖于检测对象的特征，即通过提前分析恶意行为来定义危险信号。

例如，在对僵尸网络进行检测的过程中[12]，根据僵尸主机所具有的信息窃取、频繁与僵尸控制者通信等恶意行为特点，将 PAMP 信号定义为每秒连续调用击键函数的次数，以捕获受感染的僵尸主机进行键盘扫描的恶意行为；危险信号定义为网络数据接收和发送的时间差，以寻找频繁访问网络资源的可疑行为；安全信号则定义为两次连续调用通信函数的时间间隔。从以上列举的危险理论应用中可以看出，危险信号的定义依赖于人工经验，根据恶意行为特征来确定信号的描述对象和取值范围。以这种方式定义的危险信号往往只能针对特定的危险行为，既缺乏多样性，又缺乏自适应性。该方法是一种“亡羊补牢”式的检测方法，难以检测未知危险模式，削弱了危险理论的智能性。

2.2 危险信号难以完全覆盖危险行为

针对危险信号的定义，除了信号定义过程中依赖于先验知识外，还存在危险信号覆盖的完备性问题。恶意行为是复杂的，其通过对各种系统资源的调用来完成特定的功能，因此，在计算机系统中，需要定义多种危险信号协同作用才能发现潜在的危险[13]。例如前面所述的受感染的僵尸主机，其窃取机密数据行为的实施就包括了“键盘扫描→消息记录→连接僵尸控制主机→消息发送”等一系列步骤。因此，若危险信号定义过少，或者因为对危险特征分析不足导致危险信号的权值设置不当，都可能忽略了潜在的危险因素，而难以捕捉到危险源。除此之外，恶意行为不明显的危险也为危险信号的定义带来了困难。在实际应用中，并不是所有的攻击都会造成显著的破坏，有些攻击与正常行为区别不大，恶意行为特征不明显，诸如此类的攻击为显著危险信号的生成制造了难题。与之相反，有些危险信号并不是仅由攻击引起，它们也可能是由正常行为所引起，这些一般化的危险信号也会造成伪肯定率的升高。

综上所述，危险信号的定义是危险理论中的核心问题，但在实际应用过程中掺杂着大量的人工经验和定义，同时对所解决问题的依赖性较强，导致算法缺乏多样性、自适应性和可移植性，与计算机免疫系统所追求的自适应性和智能性相去甚远。因此，如何建立一套不依赖于先验知识、自适应的危险信号提取方法是目前危险理论迫切需要解决的问题。

3 危险信号定义问题分析

生物学家认为，免疫是机体针对外源物质的一种反应，其作用是识别和排除抗原性异物，以此来维持机体的生理平衡[14]。本文从该定义中得到启示，认为危险理论的本质是：以系统自身的健康状况为立足点，利用机体免疫系统“生理平衡”机理，以自身状态是否“失衡”来感知危险。平衡状态的打破来源于变化，危险理论就是要寻找“谁”导致了系统的变化，并分析这种变化是否对自身状态构成威胁，利用这种“感受”来感知危险、学习危险的特征。

3.1 问题存在的原因

本文第 2 节中介绍了危险信号定义中存在的两大问题，即危险信号的人工定义和覆盖问题。本文认为危险信号定义中这两个问题的产生主要源于以下几点原因。

(1)抗原空间的海量性：信息系统的开放性和动态特性决定了问题对象的海量性，导致危险分析和提取过程的复杂性。在实际应用环境中，由于环境的复杂性难以理清危险相关因素之间的关系，因此，只有求助于人工经验来缩小抗原空间，剔除无关因素来进行安全分析。

(2)危险行为的特异性和不确定性：信息系统是个高度开放的系统，在运行过程中面临着各种各样来自内部和外部的安全威胁，这些入侵的目的不同、功能不同、行为也不同。因此，在使用危险理论防御对信息系统进行防御时，对于何为危险缺乏统一定义，往往需要针对特定的问题对象给出危险的定义。

(3)危险信号种类的多样性：生物免疫系统中，将危险信号定义为危险相关分子模式(DAMPs)，它主要由病原体相关分子模式(PAMPs)和细胞内的危险物质 Alarmins 组成。危险理论认为病原体的感染总会造成同一种损伤，即非正常细胞死亡。但在信息系统中，危险行为可能导致多种不同的危险现象出现，这些危险现象是对危险行为的反应，即为信息系统中可能的危险信号。正是由于危险行为所带来的危险信号种类较多，难以定义完全，因此目前的研究者常常借助经验知识来定义危险信号。

3.2 问题的研究思路

危险理论中危险信号人工定义问题产生的关键原因是在信息系统中没有建立危险的一般性定义和描述方法，即对何为危险没有一种普适性的定义方法。因此，本文针对危险信号提取存在的两大问题，试图解决危险感知中存在的人工定义和缺乏自适应性等问题，建立一套危险感知的一般性方法。具体思路是：

(1)基于“变化导致危险”这一思想，将变化作为潜在危险信号，建立危险信号的普适性定义方法，改变目前存在的人工定义问题；

(2)根据分析对象的特征，建立相应的变化提取和变化特征分析方法；

(3)通过对变化的捕获来提取危险信号，并分析危险发生时系统的运行特征和规律，为相似危险的自适应感知提供知识和参考。

4 基于变化的危险信号自适应提取模型

4.1 模型框架

危险信号 DS(Danger Signals)是系统中各种潜在的危险因素，是进行危险分析的依据和基础，因此危险信号 DS 是各种变化的集合，即 $DS=\{dv_i \mid i\in N\}$，其中 dv_i 以微分的表达方式表示指标变量的变化，$V=\{v_i \mid i\in N\}$ 表示各级别的系统指标变量。

信息系统中求变化的方法多种多样，按照变化的差别和变化求取的方式不同，它主要可以分为两种：基于值的变化 VC(Value Changes)和基于特征的变化 FC(Feature Changes)，其中，$VC=\{vc_i \mid i\in N\}$ 表示值变化指标的集合，$FC=\{fc_i \mid i\in N\}$ 表示特征变化指标的集合。

图 1 为变化的危险信号提取模型框架，该模型主要由计算机系统各种资源状态指标的实时采集器(Resources Real-

time Collector,RRC)和变化感知器(Changes Sensor,CS)两部分组成。

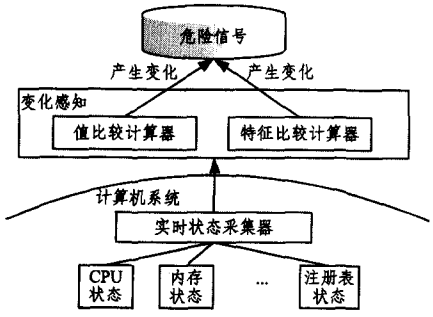

图1 基于变化的危险信号提取模型

资源实时采集器RRC的主要功能是对计算机系统中的各种关键指标的运行状态进行实时监控和采集,以供模型进行进一步分析来查找变化,它是本模型的数据来源。

变化感知器CS模块是本模型的核心部件,其主要功能是对采集器所提供的数据进行分析,寻找产生变化的指标,将其提取并作为危险信号。

输入:$INPUT=V=\{v_i \mid i\in N\}$(表示资源采集器RRC所采集到的进程、网络、系统等各级别的系统数据);

输出:$OUTPUT=DS=\{dv_i \mid i\in N\}$(输出为产生变化的指标,将这些指标定义为危险信号)。

运算方式:①基于值的变化计算(VC)={距离计算方法,夹角余弦计算方法,相关系数计算方法};②基于特征的变化计算(FC)=特征三元组比较方法。

关系:$DS=\{ds_i=dv_i \mid i\in N\}=\{vc_i \mid i\in N\}\cup\{fc_i \mid i\in N\}$,模型中输出的危险信号由值变化和特征变化方法两种方法计算所得到的变化组成。

4.2 基于值变化的危险信号提取

基于值变化的检测方法主要使用距离指数或相似性指数等指标来比较不同时段检测对象的特征差异,然后根据给定的经验阈值判断检测对象是否发生变化。常见的用于变化检测的距离指数包括欧氏距离、绝对距离、豪式距离等,利用相似性指数求变化的方法主要是使用夹角余弦和相关系数等公式进行计算[15]。常用的计算公式包括:欧氏距离、绝对距离、夹角余弦和相关系数的计算,以此来描述指标数据的变化。

基于欧氏距离计算变化:

$$vc=\sqrt{\sum_{i=1}^{n}(x_{ri}-x_{ti})^2} \tag{1}$$

基于绝对距离计算变化:

$$vc=\sum_{i=1}^{n}|x_{ri}-x_{ti}| \tag{2}$$

基于夹角余弦计算变化

$$vc=\frac{\sum_{i=1}^{n}x_{ri}\cdot x_{ti}}{\sqrt{\sum_{i=1}^{n}x_{ri}^2\cdot\sum_{i=1}^{n}x_{ti}^2}} \tag{3}$$

基于相关系数计算变化:

$$vc=\frac{\sum_{i=1}^{n}(x_{ri}-\overline{x_r})\cdot(x_{ti}-\overline{x_t})}{\sqrt{\sum_{i=1}^{n}(x_{ri}-\overline{x_r})^2\cdot\sum_{i=1}^{n}(x_{ti}-\overline{x_t})^2}} \tag{4}$$

以上变化的计算公式中,x_{ri},$i\in[1,n]$表示时间窗口W内的n个需要进行比较的取值,x_{ti},$i\in[1,n]$表示时间窗口W内的n个样本点,给定变化阈值$Threshold$后,若$vc>Threshold$,则该监测指标存在变化,即为潜在危险,认为该指标产生了一个危险信号。

4.3 基于特征变化的危险信号提取

笔者在文献[16]中提出了通过比较系统变量运行特征来检测变化的方法,利用各种系统资源采集器对目标系统或软件运行时资源占用情况的采集,刻画出系统资源的运行情况,总结出运行趋势。通过对软件正常运行时和非正常运行时资源变化情况的比较来感知和捕捉变化。

计算机系统中,软件的运行情况有其固有的特征,在软件进行大量数据计算时,往往会带来资源占用率的大量增加,此时虽然各种指标大幅增加,但其整体运行特征并未发生变化,即资源占用的特征规律未发生改变。若采用值比较的变化检测方法,这种由大数据量运算带来的资源占用率的大量增加,会导致检测值大于经验阈值而造成误判。基于特征的变化描述方式FC(Feature Changes)可以较好地弥补这种缺陷,该方法采用数值微分的思想对离散数据进行了分析和描述,构建了特征描述三元组。利用数值微分方法定义三元组$\{f'(x_i)_{left},f(x_i),f'(x_i)_{right}\}$,该三元组中的$f'(x_i)_{left}$,$f'(x_i)_{right}$分别表示了特征点左边和右边曲线的趋势,类似于特征点与其时间点前、后所组成的直线的斜率,如图2所示,其中$f'(x_i)_{left}$和$f'(x_i)_{right}$分别表示两条直线的斜率。

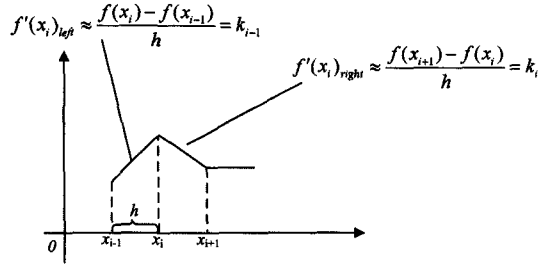

图2 特征三元组中元素特征的描述

使用该三元组能够刻画特征检测点及其与相邻点所构成的曲线的趋势,采集各个特征点所对应的三元组,就能够实现对系统资源运行情况的描述。通过对正常运行情况下和待检时计算出的三元组的比较,可实现基于特征的变化检测。

由特征检测方法计算的特征变化如式(5)所示,其中x_i和x_t分别表示检测特征点和所比较的样本特征点,$|f'(x_i)_{left}-f'(x_t)_{left}|$表示两点向左微商的差值,即特征点左部特征的变化,$|f'(x_i)_{right}-f'(x_t)_{right}|$表示特征点右部特征的变化,利用这两个差值的和来表示特征的变化。

$$fc_i=|f'(x_i)_{left}-f'(x_t)_{left}|+|f'(x_i)_{right}-f'(x_t)_{right}| \tag{5}$$

5 实验与结果分析

实验旨在以僵尸程序(SpyBot)为例,验证本文所提出的基于变化特征的危险信号提取方法的可行性和自适应性,即在不同的恶意行为条件下,不需要任何经验知识,仅从变化的角度来验证提取到的危险信号是否能够表征危险的特征;同时,随着恶意行为的变化,本方法所提取的危险信号是否能够自适应调整。

5.1 实验设计

僵尸程序具有一定的潜伏性和伪装性,特别是在僵尸主

机等待攻击者命令的潜伏期内，其恶意行为不明显，具有一定的反检测能力。但由于僵尸程序“与生俱来”的攻击性，即使处于潜伏阶段，僵尸程序也仍然会存在一定的蛛丝马迹使得被感染主机产生一定的变化。本文所提变化检测方法的特点就是从变化入手来感知危险，本实验将通过检测被监测主机上各种性能指标的变化来感知主机系统中存在的异常和危险，从而捕捉潜伏在主机上的僵尸程序。

表1 采集指标列表

指标类型	指标名称	指标描述
系统级	PID	进程号
	P_name	进程名
	P_num	系统进程数量
	P_cpu	进程的CPU占用率
	P_mem	进程的内存占用率
网络级	HTTP_Packets	每秒内发送/接收到的HTTP包数量
	TCP_Packets	每秒内发送/接收到的TCP包数量
	UDP_Packets	每秒内发送/接收到的UDP包数量
	ARP_Packets	每秒内发送/接收到的ARP包数量
	ICMP_Packets	每秒内发送/接收到的ICMP包数量
	IRC_Packets	每秒内发送/接收到的IRC包数量

本次实验采集的数据包括系统级和网络级的指标，共11个，采集周期为1s。表1列出了采集的系统指标。

5.2 实验分析

在本次试验中，采集到的TCP、ARP和UDP数据包变化频率较大，但其数据包取值固定，因此采用值比较的方法来检测变化，其余均采用特征比较的方法进行变化的检测。

从表2的结果可以看出，实验系统根据每种恶意行为操作时的特点，自动提取危险信号，其中IRC和P_mem的变化最为剧烈。以在僵尸程序潜伏阶段所采集到的危险信号为例，提取到的危险信号为IRC和P_mem，这是由于此时僵尸程序虽然处于潜伏阶段，但仍然会利用IRC协议与攻击者频繁联系，因此会带来一些数据包的变化，同时IRC通信客户端进程mirc.exe的内存占用量也明显增加。从这些自动筛选出来的危险信号可以看出，不同的恶意行为会带来不同的指标变化，表明了以变化检测危险这一方法具备多样性和智能性。同时，由于恶意潜伏软件本身的特点，这些自适应提取的危险信号也在一定程度上代表了危险的特征。

表2 僵尸程序危险信号生成情况表

	僵尸程序潜伏阶段	僵尸程序被唤醒	僵尸执行键盘记录指令	执行删除进程指令	停止恶意行为	退出僵尸程序
时间	07:29～08:25	08:26～09:46	09:47～10:42	11:48～14:18	15:28～16:20	16:21
突变次数	TCP:0 ARP:0 UDP:0 IRC:4 P_mem:3 P_cpu:0 P_num:1	TCP:0 ARP:0 UDP:0 IRC:4 P_mem:2 P_cpu:0 P_num:0	TCP:0 ARP:0 UDP:0 IRC:3 P_mem:1 P_cpu:0 P_num:0	TCP:0 ARP:0 UDP:0 IRC:6 P_mem:6 P_cpu:1 P_num:1	TCP:0 ARP:0 UDP:0 IRC:1 P_mem:1 P_cpu:0 P_num:0	TCP:0 ARP:0 UDP:0 IRC:1 P_mem:0 P_cpu:0 P_num:0
危险信号	IRC P_mem P_num	IRC P_mem	IRC P_mem	IRC P_mem P_cpu P_num	IRC P_mem	IRC

结束语 危险理论作为人工免疫学的一个重要研究分支，在入侵检测、数据挖掘等领域的应用取得了许多成果。危险信号的定义作为危险理论应用的核心问题之一，目前主要依赖于人工经验，尚缺乏统一的描述和定义方法。本文从“变化感知危险”这一思想出发，提出了一套基于变化特征的危险信号自适应提取模型。该模型通过捕捉系统中的变化，在不依赖于人工经验和先验知识的情况下实现了危险信号的提取，本文用实验初步验证了该模型的有效性和自适应性。在本文所构建的模型进行变化分析的过程中引入了值比较和特征比较两种方法来提取变化，但哪种指标更适合哪种比较方法还需要通过大量的实例来进行验证和分析，以期建立更完善的危险信号自适应提取方案。

参 考 文 献

[1] Aickelin U, Cayzer S. The Danger Theory and Its Application to Artificial Immune Systems [C]// Proceedings of the 1st International Conference on Artificial Immune Systems (ICARIS-2002). Canterbury, UK, 2002: 141-148

[2] Vella M, Roper M, Terzis S. Danger Theory and Intrusion Detection: Possibilities and Limitations of the Analogy[C]// Proceedings of the International Conference on Artificial Immune Systems(ICARIS-2010). 2010: 276-289

[3] Greensmith J, Aickelin U. Dendritic Cells for SYN Scan Detection[C]// Proceedings of 9th Annual Conference on Genetic and Evolutionary Computation. 2007: 49-56

[4] Zhu Y, Tan Y. A Danger Theory Inspired Learning Model and Its Application to Spam Detection[C]// Advances in Swarm Intelligence: Proceedings of 2nd International Conference on ICSI 2011. Springer, 2011: 382-389

[5] Musselle C. Rethinking Concepts of the Dendritic Cell Algorithm for Multiple Data Stream Analysis[C]// Proceedings of the 11st International Conference on Artificial Immune Systems (ICARIS-2012). Berlin Heidelberg, 2012: 246-259

[6] Gu F, Greensmith J, Aickelin U. The Dendritic Cell Algorithm for Intrusion Detection [M]// Biologically Inspired Networking and Sensing: Algorithms and Architectures. 2012

[7] Vella M, Roper M, Terzis S. Danger Theory and Intrusion Detection: Possibilities and Limitations[C]// Proceedings of 9th International Conference on Artificial Immune Systems (ICARIS 2010). 2010: 276-289

[8] Bianchi M E. DAMPs, PAMPs and alarmins: all we need to know about danger [J]. Journal of Leukocyte Biology, 2007, 81 (1): 1-5

[9] Greensmith J, Aickelin U. Dendritic Cells for SYN Scan Detection [C]// Proceedings of 9th Annual Conference on Genetic and

Evolutionary Computation. 2007:49-56

[10] Greensmith J, Aickelin U, Twycross. Articulation and Clarification of the Dendritic Cell Algorithm [C]// Artifical Immune Systems: Proceedings of the 5th International Conference on Artificial Immune Systems(ICARIS). Springer, 2006:404-417

[11] Oates R, Greensmith J, Aickelin U, et al. The Application of a Dendritic Cell Algorithm to a Robotic Classifier [C]// Artificial Immune Systems: Proceedings of 6th International Conference on ICARIS 2007. Springer, 2007:204-215

[12] Al-Hammadi Y, Aickelin U, Greensmith J. DCA for bot detection [C]// Evolutionary Computation(CEC 2008). 2008:1807-1816

[13] Vella M, Roper M. Characterization of a danger context for detecting novel attacks targeting Web-based systems [EB/OL]. http://www.cis.strath.ac.uk/~mv/trep2.pdf. 2010

[14] 陈慰峰. 医学免疫学[M]. 北京:人民卫生出版社, 2000
Chen Wei-feng. Medical Immunology [M]. Beijing: People's Medical Publishing House Press, 2000

[15] Li Y, Chen J, Gong P, et al. Study on Land Cover Change Detection Method Based on NDVI Time Series Datasets Change Detection Indexes Design [J]. Journal of Basic Science and Engineering, 2005, 13(3):261-275

[16] Yang Chao, Liang Yi-wen, Liu Ao-lin. The Danger Sensed Method by Feature Changes [J]. Energy Procedia 13, 2011:4429-4437

(上接第 160 页)

参 考 文 献

[1] Fazio P, De Rango F, Lupia A. A new application for enhancing VANET services in emergency situations using the WAVE/802.11p standard[C]// Wireless Days(WD), 2013 IFIP. IEEE, 2013:1-3

[2] 乔震,刘光杰,李季,等. 移动自组织网络安全接入技术研究综述[J]. 计算机科学, 2013, 40(12):1-8, 30
Qiao Zhen, Liu Guang-jie, Li Ji, et al. Survey on Secure Access Technology in Mobile Ad-hoc Network[J]. Computer Science, 2013, 40(12):1-8, 30

[3] Sharma S, Mishra R, Kaur I. New trust based security approach for ad-hoc networks [C]// 2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT). Chengdu, 2010, 9:428-431

[4] Xia H, Jia Z, Sha E H M. Research of trust model based on fuzzy theory in mobile ad hoc networks[J]. IET Information Security, 2013, 8(2):88-103

[5] 陈深龙,张玉清. 增强 ad hoc 网络可生存性的健壮多维信任模型[J]. 通信学报, 2010(5):1-9
Chen Shen-long, Zhang Yu-qing. Robust multi-dimensional trust model for improving the survivability of ad hoc networks[J]. Journal on Communications, 2010(5):1-9

[6] Amaresh M, Usha G. Efficient malicious detection for AODV in mobile ad-hoc network[C]// IEEE International Conference on Recent Trends in Information Technology(ICRTIT). Chennai, 2013:263-269

[7] Bhoi S K, Nayak R P, Dash D, et al. RRP: A robust routing protocol for Vehicular Ad Hoc Network against hole generation attack[C]// IEEE International Conference on Communications and Signal Processing (ICCSP). Melmaruvathur, 2013: 1175-1179

[8] Bao F, Chen R, Chang M J, et al. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection[J]. IEEE Transactions on Network and Service Management, 2012, 9(2):169-183

[9] Josang A, Knapskog S J. A metric for trusted systems[C]// Proceeedings of the 21st National Security Conference. 1998:16-29

[10] 胡玲珑,潘巨龙,崔慧. 无线传感器网络中基于信誉的恶意节点检测方法[J]. 中国计量学院学报, 2012, 23(1):41-47
Hu Ling-long, Pan Ju-long, Cui Hui. A reputation-based method for detecting malicious nodes in WSNs[J]. Journal of China Jiliang University, 2012, 23(1):41-47

[11] Theodorakopoulos G, Baras J S. On trust models and trust evaluation metrics for ad hoc networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2):318-328

[12] Jiang T, Baras J S. Trust Evaluation in Anarchy: A Case Study on Autonomous Networks[C]// INFOCOM. Barcelona, Spain, 2006

[13] Ding Q, Li X, Jiang M, et al. Reputation-based trust model in vehicular ad hoc networks[C]// IEEE International Conference on Wireless Communications and Signal Processing (WCSP). Suzhou, 2010:1-6

[14] Saraswat D, Chaurasia B K. AHP Based Trust Model in VANETs [C]// 2013 5th International Conference on Computational Intelligence and Communication Networks (CICN). Mathura, 2013:391-393

[15] 田俊峰,鲁玉臻,李宁. 基于推荐的信任链管理模型[J]. 通信学报, 2011, 32(10):1-9
Tian Jun-feng, Lu Yu-zhen, Li Ning. Trust chain management model based on recommendation[J]. Journal on Communications, 2011, 32(10):1-9

[16] Mui L. Computational models of trust and reputation: Agents, evolutionary games, and social networks[D]. Cambridge: Massachusetts Institute of Technology, 2002

[17] Dellarocas C. Reputation mechanism design in online trading environments with pure moral hazard[J]. Information Systems Research, 2005, 16(2):209-230

[18] 王良民,郭渊博,詹永照. 容忍入侵的无线传感器网络模糊信任评估模型[J]. 通信学报, 2010, 31(12):37-44
Wang Liang-min, Guo Yuan-bo, Zhan Yong-zhao. Fuzzy trust model for wireless sensor networks with intrusion tolerance[J]. Journal on Communications, 2010, 31(12):37-44