Journal of Computer Applications
计算机应用, 2020, 40(5): 1340 - 1347
ISSN 1001-9081
CODEN JYIIDU
2020-05-10
http://www.joca.cn

文章编号:1001-9081(2020)05-1340-08
DOI:10.11772/j.issn.1001-9081.2019091699

基于订阅/发布服务的广域信息管理系统应急响应机制

吴志军*,王　航
(中国民航大学 电子信息与自动化学院,天津 300300)
(*通信作者电子邮箱zjwu@cauc.edu.cn)

摘　要:广域信息管理系统(SWIM)是一个分布式的大型网络系统,它实时地向空中交通管理部门、航空机场和航空公司等提供不间断的航空信息数据共享和传输服务。为了保障SWIM服务的连续性,研究了基于订阅/发布服务的SWIM系统应急响应机制。首先,根据实时监测SWIM网络的各性能指标,提出了基于改进的模糊层次分析的网络可生存性评估方法;其次,当SWIM网络生存性指标下降到低于参量的边界值时,发布相应信息到订阅者,由订阅者确定是否进行服务漂移;最后,分别针对自然灾害和分布式拒绝服务(DDoS)攻击两种情况,提出了基于订阅/发布服务的SWIM应急响应模型(ERMSP),该模型以订阅发布和信任管理机制为基础。仿真实验结果表明,通过对网络性能各指标的实时监测和部署ERMSP,可抵抗性提高了8.9%,业务连续性提高了18.2%,可以实现SWIM的应急响应。

关键词:分布式系统;订阅发布;广域信息管理系统;应急响应
中图分类号:TP393; TN915.08　　**文献标志码**:A

System wide information management emergency response mechanism based on subscribe/publish service

WU Zhijun*, WANG Hang
(*College of Electronic Information and Automation*, *Civil Aviation University of China*, *Tianjin* 300300, *China*)

Abstract: System Wide Information Management (SWIM) is a distributed, large-scale network system that provides uninterrupted aviation information data sharing and transmission services to air traffic management departments, airports and airlines in real time. In order to guarantee the continuity of SWIM services, the emergency response mechanism of SWIM based on subscription/release service was studied. Firstly, by real-time monitoring various performance indicators of SWIM network, a network survivability evaluation method based on improved fuzzy analytic hierarchy process was proposed. Secondly, when the network survivability index fell below the boundary value of the parameter, the corresponding information was published to the subscriber. It was determined by the subscriber whether to perform the service migration. Finally, an Emergency Response Model based on Subscribe/Publish service (ERMSP) for SWIM was proposed for natural disasters and Distributed Denial of Service (DDoS) attacks. The model is based on subscribe, publish and trust management mechanisms. Simulation experimental results show that the resistibility is improved by 8.9% and the business continuity is improved by 18.2% by real-time monitoring of network performance indicators and deployment of ERMSP, which can realize the emergency response of SWIM.

Key words: distributed system; subscribe/publish; System Wide Information Management (SWIM); emergency response

0　引言

随着全球经济的发展,现有航空运输系统已不能满足日益增长的民航业务需求,为此,美国提出下一代航空运输系统(Next Generation Air Transportation System, NextGen),欧洲提出单一欧洲天空空中交通管理研究(Single European Sky ATM, SESAR),中国提出新一代空中交通管理系统(New Generation Air Traffic Manager, NGATM),这些计划都以广域信息管理系统(System Wide Information Management, SWIM)为基础。SWIM在全球范围内保证了空中交通管理部门、航空公司和机场等之间的信息共享,提高了协同决策能力。由于民航系统的特殊性,该系统需要提供7×24 h不间断服务,因此,研究SWIM的应急响应显得尤为重要。

本文提出了一种基于订阅/发布的SWIM应急响应机制。

1　相关工作

有关应急响应的研究工作,大致可以分为三类:关键服务漂移、可生存性和系统安全性。

Kun等[1]针对网络安全提出了基于流和应用的应急响应机制,但只对应急响应和应急措施进行了理论分析;Seba等[2]针对无线通信中的安全威胁,研究了安全需求,并提出了应急通信体系结构,但没有提供完整的各个阶段的威胁及相应的解决方案;Yeo等[3]研究快速网络评估(Rapid Network

收稿日期:2019-10-10;**修回日期**:2019-12-11;**录用日期**:2019-12-13。
基金项目:国家自然科学基金委员会与中国民航局联合基金资助项目(U1933108);中央高校基本科研业务费资助项目(3122018D007)。
作者简介:吴志军(1965—),男,新疆库尔勒人,教授,博士,主要研究方向:网络与信息安全;　王航(1992—),男,河北保定人,硕士研究生,主要研究方向:广域信息管理、信息安全。

Assessment, RNA)和手册内容分析(Manaual Content Analysis, MCA)两种编码方式的优缺点,这两种方法能提高应急响应行动的效率,证明了MCA在实时网络中的可用性,但是没有给出两种方式的具体适用范围;Wang等[4]研究了突发灾害情况下消息的开销、延迟和路由问题,提出了一种传播转发路由算法和动态拓扑建模方法,设计了传播策略和转发策略;Wu等[5]针对SWIM的生存性提出了一种动态迁移机制,并且与随机自治可生存调度(Stochastic Autonomous Scheduling Survivability, SASS)模型和基于令牌的竞争机制(Token-based competition mechanism,TOKEN)模型对比,具有优越性,但只考虑了关键服务迁移机制,无法完全满足SWIM的应急响应。

Dalal等[6]研究了灾害位置不确定情况下的应急网络的设计,研究了最坏情况和最小成本下不同权重的分配问题,从而提高该方案的效率,而且进行了实例研究,但是并没有考虑其他不确定性因素,如基础设施的损坏、人员的撤离等;Vedula等[7]以一个应急响应案例为基础研究了信任机制的影响,但是没有把时间因素考虑进信任机制中;Qiu等[8]研究了物联网的实时应急响应能力,提出了应急响应路由协议来提高数据传输效率,但是没有考虑到大型的系统;Es-Haghi等[9]使用模糊方法和社会网络分析来进行应急响应,并且考虑了预测方法来实现理想的应急管理目标,但考虑的变量不多,应考虑加入更多的变量;Qiu等[10]提出了应急贝叶斯决策网络(Emergency Bayesian Decision Network, EBDN)模型来应对突发事件决策问题,解决了突发事件中的不确定性,但是该方法依赖于一定的历史数据,并且没有考虑突发事件的派生事件;Gu等[11]研究了多种信息系统间的基础架构,构建了应急响应拓扑,但是没有进一步因灾难的不同而变换的网络拓扑;Lieser等[12]研究了移动自组织网络中信息优先级的问题,从而降低了网络延迟,提出的体系结构在灾后通信方面作出重大贡献;王健等[13]提出了一种基于SM-PEPA(Semi-Markov Performance Evaluation Process Algebra)系统的量化分析方法,将系统认知能力转化为一个半马尔可夫过程,但是仅考虑了入侵防御能力和自恢复成功率对可生存性的影响;王鹏飞等[14]从软件、硬件和运行环境3个因素层提出一套指标体系来量化可生存能力,但其一级指标的权值选取方法有待优化,二级指标采用均值加权法也不合理;陈天平等[15]提出一种可生存性评估方法,给出了指标量化方法,但其权重系数简单地采用相同的值,这与实际情况不符。

Kang等[16]从信息集成的角度研究了SWIM;Qi等[17]概述了SWIM并且进行了安全性分析;Abraham[18]研究了空地SWIM,考虑了航空器接入SWIM;Morioka等[19]为了完成航空器和空中交通管理间丰富的信息交换,研究了航空移动式机场通信系统;Moallemi等[20]研究了航空器接入SWIM的信息安全问题;Wilson等[21]研究了SWIM的信息安全问题;Wang等[22]提出了基于面向服务架构(Service-Oriented Architecture, SOA)的SWIM架构;赵汨龙等[23]提出了一个基于SOA的SWIM框架下的实现实例;袁飞飞等[24]提出了协同的数据分发方法以应对大数据量的分发效率,在订阅/发布模式下,降低了分发时延,减轻了节点负载。

基于以上研究现状,本文提出的基于订阅发布服务的SWIM应急响应机制弥补了以往研究的不足,提高了SWIM的可生存性。

2　SWIM应急响应机制

SWIM的范围包括基础设施、信息、服务和治理,为顶层SWIM支持的服务提供技术支持。SWIM是网络层和应用层之间的大规模分布式网络,其应急响应体系结构如图1所示。

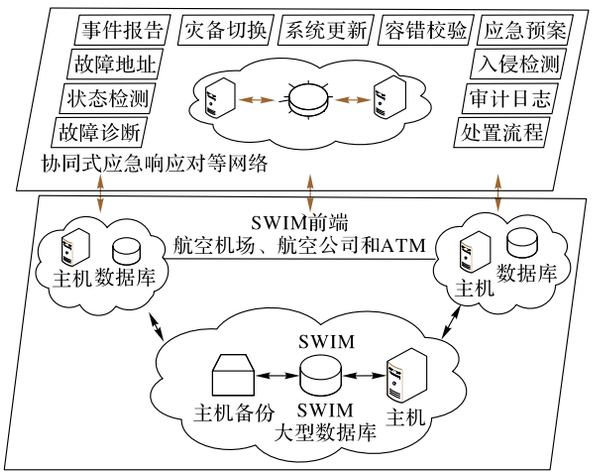

图1　SWIM应急响应体系结构

Fig. 1　SWIM emergency response architecture

SWIM应急响应体系结构分为协同式应急响应对等网络(Peer-to-Peer,P2P)和SWIM物理网络两层,在协同式对等网络中,各实体间平等、协同地完成信息地共享,这与SWIM的应急响应模式非常相似,所以可以兼容SWIM的组织架构。通过P2P网络,可以实现SWIM应急消息的快速发布,提供的功能包括:事件通告、灾备切换、故障地址、状态监测、故障诊断、系统更新、容错校验、应急预案、安全更新、入侵检测、审计日志和处置流程等。

在SWIM应急响应体系中需各部门协同运行,即两个或更多成员之间共同完成应急响应,包括信息共享、共同的应急响应流程和紧急情况下系统运行等。通过机场、航空公司和空管等各方参与和信息共享更好地进行应急响应,目标是:1)增加共同的态势感知;2)多方参与,提高应急响应能力;3)协同响应,提高资源利用率;4)加强协同配合。

2.1　SWIM的应急现有模型

SWIM全球互操作框架包括5层,自上而下依次是:应用层、信息交换服务层、信息交换模型层、SWIM基础设施层和网络连接层,其中,SWIM的范围包括信息交换服务层、信息交换模型层和SWIM基础设施层,以及对这些在安全等方面的治理。当SWIM受到分布式拒绝服务攻击(Distributed Denial of Service, DDoS)时,不同层会有不同的应急响应机制。

在协同式应急响应服务对等网络基础上,设计了SWIM应急响应模型,如图2所示,由分布数据存储层、分层动态漂移系统和网络连接层构成。实现SWIM网络关键服务的动态漂移和关键数据的备份以及恢复。

在信息交换服务层中,首先设置各个服务的权值,把关键服务和普通服务区分开来,以机场订阅的相关服务为例,当受到DDoS攻击时,机场所订阅的相关服务只会保留关键服务而普通服务会暂时停止,权值被设为零。

在信息交换模型层中,信息交换模型规定了发布者和订阅者之间传递消息的结构、格式和内容,包括信息域的概念。现有信息交换模型有航空信息交换模型(Aeronautical

Information eXchange Model, AIXM)、航班信息交换模型(Flight Information eXchange Model, FIXM)和气象交换逻辑模型(Weather eXchange Logical Model, WXXM)。各个模型分别包含概念模型、逻辑模型和可扩展标记语言(eXtensible Markup Language, XML)模型。以FIXM为例,核心数据包含整个生命周期中的计划、状态以及应急数据等基本信息和关键数据,FIXM的拓展部分可由各个国家和地区根据自身具体情况进行调整。发生DDoS攻击时,该模型会简化为只保留核心部分的简化模式,以保证SWIM业务的连续性。

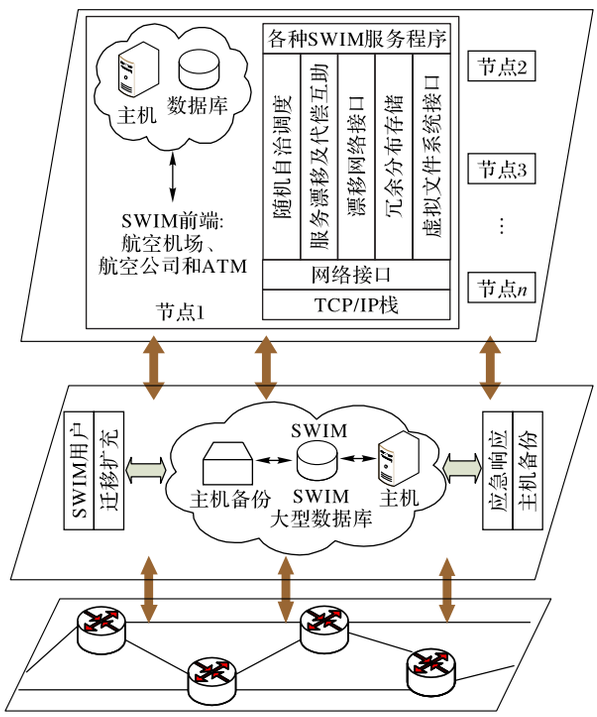

图2 应急响应模型

Fig. 2 Emergency response model

在SWIM基础设施层提供SWIM的核心服务,包括消息服务、接口服务、安全服务和企业服务管理等。消息服务为SWIM提供高效、安全可靠数据传送,包括发布/订阅、请求/响应、消息路由和消息转换功能;接口管理能对SWIM中业务数据的服务元数据的注册、发布、发现和调用进行统一的管理,有利于各服务间高效的互操作和复用;安全服务主要包括安全策略、认证管理、访问控制和服务监控。安全性体现在数据的机密性、完整性、不可否认性、身份认证和访问控制等多个方面。企业服务管理主要包括策略实施/指标收集、性能监控/报告、故障检测/报告、异常反馈/告警,保证基于SOA架构的SWIM正常工作。当受到DDoS攻击时,基础设施层会临时扩容带宽,本地或运营商进行流量清洗。

SWIM基础设施层及故障转移如图3所示。

每个服务器上有一个或多个主题,并且服务器的编号不重复;发布者和订阅者通过主题互相交互,消息的主题包含不同的数据:航行情报数据、航空气象数据和空域流量数据等。订阅者可以订阅不同的主题;每个主题可以有多个分区,分区互为备份,既可以提高系统的吞吐量,也可以在服务器受到DDoS攻击时保证业务的连续性。发布者首先将主题发布到主分区中,从分区会自动跟主分区同步。首先获取服务器中的主分区,发布者将消息发送给主分区,主分区将消息写入本地文件,从分区同步主分区中的主题,同时向主分区发送确认字符(Acknowledge character, ACK),主分区收到所有副本的ACK后向发布者发送ACK。

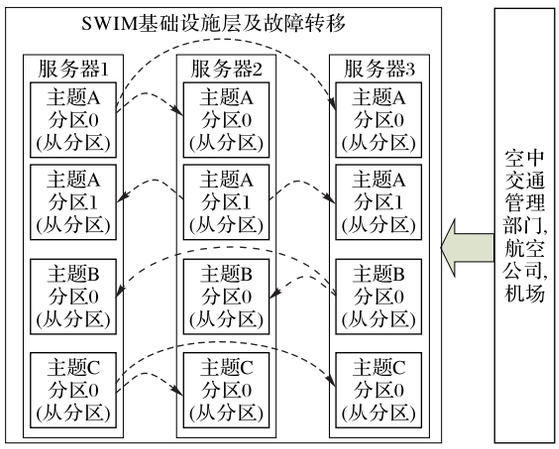

图3 SWIM基础设施层及故障转移

Fig. 3 SWIM infrastructure layer and failover

故障转移指的是当SWIM服务器受到DDoS攻击时,SWIM基础设施层可以迅速检测到该失效,并立即将服务自动转移到其他服务器上,故障转移是通过"心跳"机制完成的,只要主服务器和备份服务器间的心跳无法维持,就认为主服务器已无法正常工作,系统就会自动启动备份服务器代替主服务器。

2.2 SWIM订阅/发布核心服务模型

订阅/发布是一种可靠地传送消息的方式,其可伸缩性大。生成消息的提供者发布该消息,需要该消息的其他应用则订阅对应的主题。当发生灾难时,发布者和订阅者仍能发布及订阅事件,即故障是透明的,系统恢复正常后,达到一致的状态,保证了SWIM业务的连续性。订阅/发布系统完成了发布者和订阅者之间的通信解耦,包括:空间解耦、时间解耦和同步解耦。

与传统的点对点消息传输模式不同,在SWIM中,采用一对多的消息传输模式,发布者可以向多个订阅者进行广播。发布者和订阅者通过主题互相关联,如发布者可以发布航空信息、气象信息和航班信息,订阅者则订阅相应主题。

定义1 主题。一个主题是一个6元组,即$\langle p, s, c, con, r, tc\rangle$,其中:$p$是发布者,$s$是订阅者,$c$是主题的内容,$con$是订阅者是否处于连接状态,$r$为订阅者是否成功接收到订阅内容,$tc$是消息在主题中最大的存活时间。$con$、$r$、$tc$为布尔值;$tc$是一个范围,上限为消息发布时间,下限为消息失效时间。只有在有效期范围内,SWIM消息服务器才会发送主题给相应订阅者。

在一个主题的生命周期内有5种不同的状态:

1)订阅(subscription, sub)。SWIM消息服务器记录相应订阅者的信息及其订阅的主题。

2)待发布(pending release, per)。主题处于待发布状态,con为false,r为false,tc为false。

3)发布(publish, pub)。发布者将主题发布到SWIM消息服务器,同时主题T中的p和s也已确定,通过授权和认证,处于活跃状态的订阅者会接收到已订阅的主题。con为true,r为true,tc为true。

4)等待(wait, wat)。在主题的存活时间范围内,消息会一直存在。当已订阅了主题处于非活跃状态的订阅者变为活跃状态时,仍然能够接收该消息。此时,con为false,r为false,tc为true。

5)过期(expired,exp)。此状态主题已过期,订阅者不会收到相应消息。*con*为true,*r*为false,*tc*为false。

主题的生命周期图如图4所示。订阅者订阅主题*T*,于是主题*T*中的订阅者*s*确定,该主题成为被订阅的状态;发布者*p*确定后,主题进入待发布状态;发布者发布主题后,处于活跃状态的订阅者会接收到相应消息,此时*con*、*t*和*tc*都为true;然后主题会存活一段时间,主题处于等待状态,此时,当未连接的订阅者连接时,依然能够收到消息;当超过主题的最大存活时间时,进入过期状态,此时订阅者不会收到消息。

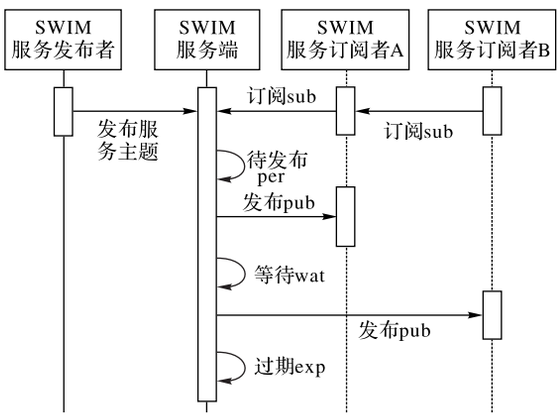

图4　主题的生命周期图

Fig. 4　Subject life cycle diagram

定义2　主题簇。一个主题簇由一组相关主题构成,$TC=\langle tt,a,s,s_0,f,s_1\rangle$,其中:$tt=\{t_1,t_2,\cdots,t_n\}$是一个有限的主题集合;*a*是发布订阅系统中的动作,包括发布publish(*publisher*,*T*,*c*,*tc*)和订阅subscribe(*subscriber*,*t*);*s*是一个有限状态集合,由*tt*中各个主题的状态决定;s_0为各个主题的初始状态;*f*为主题的状态变化函数;s_1为各个主题的最终状态。

SWIM注册库可以实现服务的管理、存储和共享。SWIM授权相关服务并发布政策和标准,包括空中交通管理参考模型(ATM Information Management,AIRM)、航班信息交换模型(FIXM)和气象交换逻辑模型(WXXM)。服务提供者发布以及提供服务,消费者发现并消费服务。

图5描述了SWIM的发布订阅模式与注册库的关系。主题的生产者将主题发布到注册库中,被订阅的主题就会推送到相应的消费者,每当有主题有更新时,相应的订阅者都会收到更新后的主题,从而大大提高发布订阅的效率。例如:订阅者1、2和3同时订阅了航班信息主题簇,注册库中相应主题就变为了已订阅状态,*tt*中包含航班信息主题簇中的各个主题,*a*的动作会从发布变为订阅。订阅者可以订阅不同的主题簇以满足自身的不同需求。

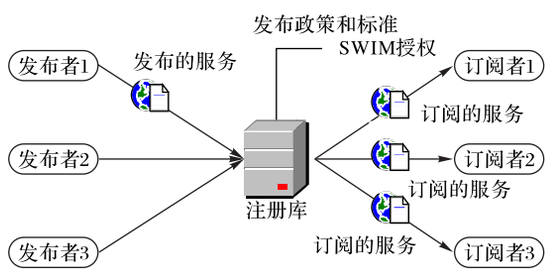

图5　SWIM的发布订阅模式及注册库

Fig. 5　SWIM's publish and subscribe mode and registry

2.3　SWIM的应急响应流程

SWIM应急响应流程(如图6所示)包括:灾前的备份系统、灾中的漂移系统和灾后的恢复系统。这里,主要考虑受到DDoS攻击的情况。在灾前的备份系统中,采用本地备份和异地备份相结合的方式,当受到攻击时,关键服务会自动切换到异地备份系统中。当SWIM生存性降低到一定程度,系统采用基于信任值的Viterbi算法进行服务漂移。

SWIM的应急响应流程的具体步骤如下:

1)在SWIM中,首先要确定关键服务,包括航班信息服务,航空信息服务和气象信息服务,当系统受到攻击时,保证关键服务不中断。然后评估各关键服务的生存指标,并且评估系统服务的态势,SWIM监控部门负责查看可生存性、可抵抗性等网络性能是否下降到参量的边界值。

2)指标超过了边界值,判断受影响的业务,包括航空信息服务、航班信息服务、气象信息服务他其他服务,然后将应急响应消息发布到利益相关者及应急响应小组,应急响应小组采取应急措施。

3)判断服务是否需要漂移,如果需要漂移,采取应急响应措施,根据基于信任值的Viterbi算法进行服务漂移,保证业务的连续性,然后上调服务器的信任值。当不需要漂移时,查看服务是否已完成,如果完成,上调信任值,否则下调信任值。

4)回到系统地初始部分,即监控个关键服务的生存性指标。

此应急响应流程指明了从应急事件开始到应急事件结束时的详细流程,为SWIM的应急响应奠定了基础。依据此流程,应急响应的各个动作可有条不紊地进行。

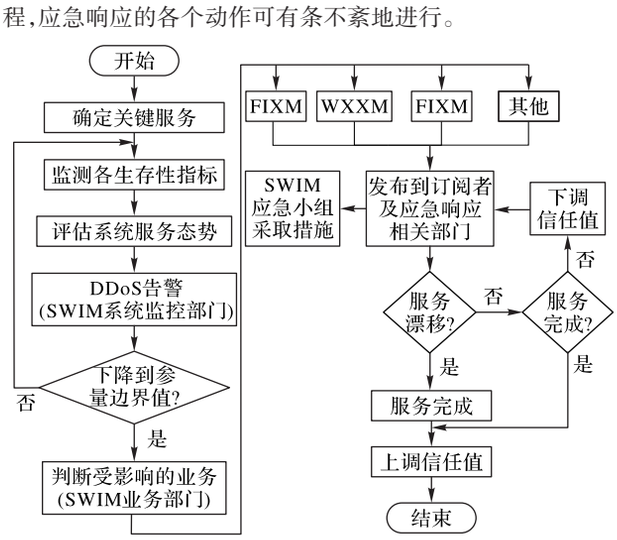

图6　应急响应流程

Fig. 6　Emergency response process

2.4　应急响应能力指标

本文评估SWIM的应急响应能力通过3个评价指标来实现:可识别性、可抵抗性和业务连续性。

可识别性是指当系统遭受自然灾害或者DDoS攻击时,系统识别异常的能力。系统可识别性越高,及时发现异常情况越早,对SWIM系统业务的影响就越小,损失就能降到最低。通过本文提出的基于订阅/发布服务的SWIM应急响应模型(Emergency Response Mechanism based on Subscribe/Publish,ERMSP),自适应地调整可识别性参数,参数与观察变量的概率分布是一一对应的。

可抵抗性是指当突发事件来临时,关键业务不受影响,系

统继续提供服务的能力，其中，关键服务包括航班信息服务、航空信息服务和气象信息服务等。可抵抗性是SWIM应急响应能力的一项重要指标，可抵抗性越强，应急响应能力越强。可抵抗性通过网络性能变化的快慢来体现。业务连续性是指SWIM业务的功能是否正常，服务质量下降多少，缩短业务恢复正常的时间就是业务连续性的目标。业务连续性的目标是在任何时候、任何情况下都保证SWIM关键服务的不中断，它是一种预防机制。业务连续性的前提是要系统要有备份系统，包括本地备份和异地备份，否则连续性就无从谈起。业务连续性覆盖了整个SWIM的技术以及操作方式，它是一种计划和执行过程组成的策略。

3 仿真实验及结果分析

3.1 仿真环境和评定指标

SWIM应急机制的仿真环境如图7所示。空管、航空公司和机场等部门订阅相应主题。其中，订阅者也可作为发布者。相关主题包括航班、气象、航空、环境、流量和监控等，当节点受到攻击（DDoS攻击）等异常情况时，SWIM的核心服务服务会根据信任值（Trust Value，TV）采用Viterbi算法进行服务的漂移，从而保证业务的连续性。

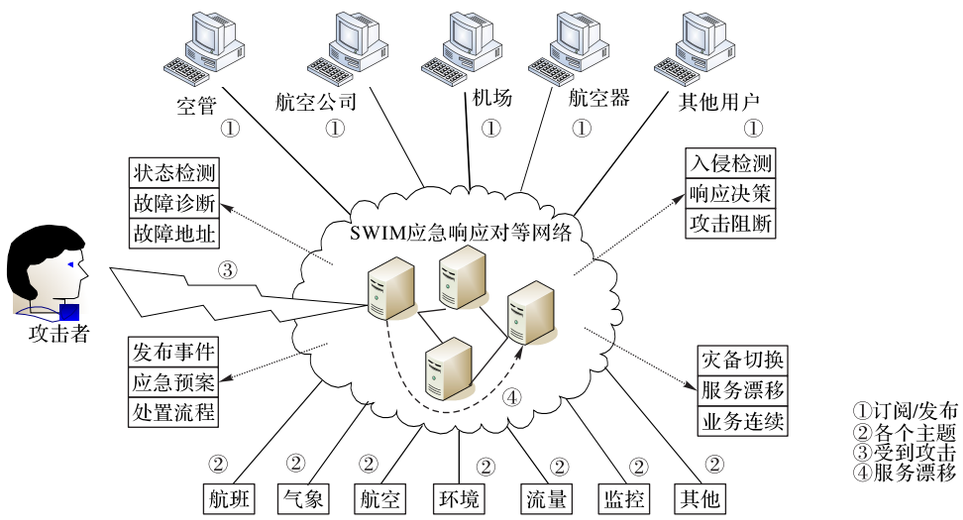

图7 SWIM实验环境

Fig. 7 SWIM experimental environment

仿真平台由计算机、服务器和路由器组成，其中，5台计算机模拟发布者和订阅者，3台计算机模拟服务器，提供SWIM服务，包括服务的注册、发布和订阅。具体配置如表1所示。

表1 仿真实验计算机硬件配置

Tab. 1 Computer hardware configurations in simulation experiments

名称	操作系统	处理器	内存/GB
计算机1（空管）	RHEL 7	i5-2450 2.5 GHz	4
计算机2（航空公司）	RHEL 7	i5-2450 2.5 GHz	4
计算机3（机场）	RHEL 7	i5-2450 2.5 GHz	4
计算机4（航空器）	RHEL 7	i5-2450 2.5 GHz	4
计算机5（其他用户）	RHEL 7	i5-2450 2.5 GHz	4
航班信息服务	Ubuntu 14.04	i5-4590 3.30 GHz	2
气象信息服务	Ubuntu 14.04	i5-4590 3.30 GHz	2
航空信息服务	Ubuntu 14.04	i5-4590 3.30 GHz	2

然后配置SWIM服务动态网站架构，具体配置为：系统采用RHEL7；服务器采用Nginx；数据库采用MySQL；脚本语言采用PHP。系统可以选用RHEL、CentOS、Fedora或Ubuntu等，这里选用RHEL7；Nginx是一款优秀的轻量级服务程序，支持热部署技术，可以7×24 h不间断提供服务；MySQL是最常用的关系型数据库之一，具有非常优秀的稳定性和安全性；PHP是Web开发领域最常用的语言之一，具有开源、免费、效率高等特性。

信任值TV是对节点可靠性的评价，$TV\in[0,1]$：当TV=1时，表明此节点可靠，可以作为漂移备选节点；当TV=0时，此节点为不可靠节点，服务漂移时不会考虑；当$TV\in(0,1)$，漂移系统会以1－TV的概率对节点进行检验，然后依据Viterbi算法选择目标节点。当服务正常完成时信任值会增加，否则会下降。如图8所示，两种线型“+”和“*”分别表示信任值上升和下降的情形，默认初始信任值都是0.5。“+”表示信任值上升，随着SWIM中各个服务的不间断运行，中间节点的信任值会不断提升，最终信任值到达1后，成为可靠的节点，当攻击或者自然灾害等异常情况发生时，会优先选择此节点作为漂移目标。同理，“*”表示信任值下降的情形，关键服务受到影响，信任值会下降，变为0后就是不可靠节点，服务漂移就不会考虑该节点。

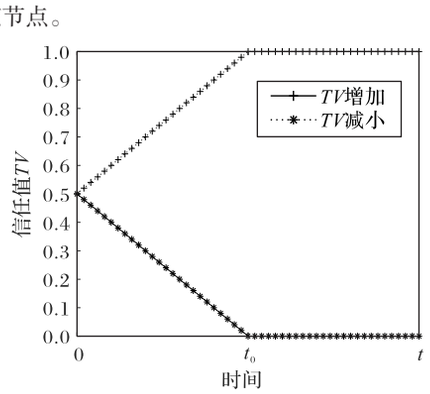

图8 信任值的变化

Fig. 8 Change in trust value

在SWIM中，面对攻击事件时，网络性能随时间的变化如图9所示。

图9所示的应急响应下的网络性能变化包括正常状态、

抵抗状态、毁伤状态、恢复状态和自适应状态5个阶段。

随着SWIM的持续运行,正常状态下的网络性能在V_1之上;当攻击或者自然灾害等异常情况发生时,网络性能逐渐下降,进入抵抗状态,下降的速率越慢,SWIM的可抵抗性越强;当系统性能下降到V_2以下,进入毁伤状态,在基于订阅/发布服务的SWIM应急响应模型中,毁伤状态下依然能够保证关键服务的连续性;SWIM中间节点漂移到信任值高的节点后,系统性能逐渐上升,进入恢复状态;当网络性能上升到V_1之上时,进入自适应状态,该状态下SWIM会对新发生的异常事件进行学习,形成一定的免疫能力,从而为下次应急响应做好充分的准备。

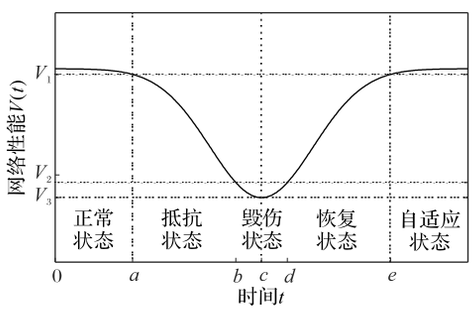

图9　应急响应下的网络性能变化

Fig. 9　Network performance changes under emergency response

系统的可识别性可通过识别时间来量化,可识别时间可通过识别的绝对时间或攻击进行的步骤计算,本文通过识别的绝对时间量化可识别性。式(1)中可识别性(Recognizability,REC)由识别时间t决定:当识别时间$t \leqslant \alpha$时,可识别性为1,此时系统可以及时处理突发事件,不会造成太大损失;当$t > \beta$时,已经造成了无法挽回的损失,系统可生存性为0;当$t \in [\alpha, \beta]$时,可以把可识别性REC量化为[0, 1]区间的值。

$$REC = \begin{cases} 1, & t < \alpha \\ -\dfrac{1}{\beta - \alpha} t + \dfrac{\beta}{\beta - \alpha}, & \alpha \leqslant t \leqslant \beta \\ 0, & t > \beta \end{cases} \tag{1}$$

系统的可抵抗性(Resistance,RES)对应于图1中的抵抗状态阶段,网络性能$V(t)$则代表可抵抗性。$V_t > V_1$时,可抵抗性为1,此时系统可以抵抗攻击;$V_2 \leqslant V_t \leqslant V_1$时,网络性能$V(t)$变化越缓慢,可抵抗性越强;$V_t < V_2$时,系统可抵抗性为0。

$$RES = \begin{cases} 1, & V_t > V_1 \\ \mathrm{e}^{-(\Delta V/\Delta t)}, & V_2 \leqslant V_t \leqslant V_1 \\ 0, & V_t < V_2 \end{cases} \tag{2}$$

系统的连续性(Continuity,CON)对应于图9中的a到e阶段,网络性能$V(t)$恢复正常的时间越短,连续性越好。

$$CON = \mathrm{e}^{-t}; \quad t \geqslant 0 \tag{3}$$

确定各指标的权值的步骤:分析SWIM,确定其应急响应能力指标,即可识别性、可抵抗性和业务连续性;对各指标进行两两比较,根据各指标的重要程度进行标度,依据表2确定模糊判断矩阵;计算各指标的权重。

表2　模糊判断矩阵的标度和含义

Tab. 2　Scales and meanings of fuzzy judgment matrix

定义	标度	含义
两两元素相比较	0.5	同等重要
两两元素相比较	0.6	前者比后者稍微重要
两两元素相比较	0.7	前者比后者明显重要
两两元素相比较	0.8	前者比后者特别重要
两两元素相比较	0.9	前者比后者极端重要
反比较	0.1,0.2,0.3,0.4	若元素a_i与a_j相比较判断为a_{ij},则元素a_j与a_i相比较判断为$a_{ji} = 1 - a_{ij}$

根据式(4)计算各指标的权重,根据式(5)判断矩阵的一致性,其中,$W_{ij} = W_i/(W_i + W_j)$, $\forall i, j \in n$,α越小,一致性要求越高。

$$W_i = \frac{\sum_{i=1}^{n} a_{ij} + \dfrac{n}{2} - 1}{n(n-1)}; \ i \in \mathbf{N} \tag{4}$$

$$\frac{1}{n^2} \sum_{i=1}^{n} \sum_{j=1}^{n} \left| a_{ij} + W_{ji} - 1 \right| \leqslant \alpha \tag{5}$$

SWIM的应急响应能力$S(T)$表示为式(6),W_T为事件T的威胁度,α,β和γ为各指标权重,且$\alpha + \beta + \gamma = 1$。

$$S(T) = (\alpha REC + \beta RES + \gamma CON) W_T \tag{6}$$

当发生了n次事件时,SWIM总体应急响应能力为:

$$S = \frac{1}{n} \sum_{i=1}^{n} S(T_i) \tag{7}$$

按照S的范围不同,安全等级可分为好、较好、正常、差和瘫痪5个等级。

3.2　ERMSP模型的对比分析

在SWIM提供正常的服务过程中,逐渐向系统中注入DDoS攻击流量,当攻击流量在20%、50%和80%时,分别监测系统的各指标状态。然后与未部署ERMSP应急响应机制的SWIM、服务随机漂移机制(Services Dynamic Migration Mechanism, SRMM)和应急贝叶斯决策网络模型(Emergency Bayes Decision Network, EBDN)对比分析,从可识别性、可抵抗性和业务连续性判断该模型是否可以满足SWIM的应急响应。表3为对各模型平均识别时间的统计,共进行了四大项实验:第一项实验是未部署ERMSP模型,分别对威胁度不同的情况下作了测试,最后得出平均识别时间为30 s;第二项实验是部署了ERMSP模型,对威胁度为0.2、0.5和0.8情形作了测试,最后得出平均识别时间为2 s;第三项实验是部署了SRMM模型,分别对0.2、0.5和0.8威胁度下作测试,得出了平均识别时间为16 s;第四项实验部署了EBDN模型,也是对威胁度为0.2、0.5和0.8进行了测试,得出平均识别时间为9 s。

SWIM的可抵抗性主要通过系统的吞吐量变化来判断,如图10所示,吞吐量变化得越慢,说明SWIM的可抵抗性越强。

表3 SWIM攻击平均识别时间对比

Tab. 3 Average recognition time comparison of SWIM attack

实验项目	威胁度	平均识别时间/s
未部署ERMSP	0.2/0.5/0.8	30
部署ERMSP	0.2/0.5/0.8	2
SRMM	0.2/0.5/0.8	16
EBDN	0.2/0.5/0.8	9

实验统计了时间从0~100 min四种模型下系统的吞吐量变化情况。在开始的30 min内，SWIM正常提供订阅/发布服务，4种模型下，吞吐量差别不大，均在500 Byte/s附近。在30 min时，向该系统中注入DDoS攻击流量，由图10可知："+"线型代表的ERMSP模型下，系统的吞吐量变化最小，仅有略微的下降，40~100 min的平均吞吐量在480 Byte/s附近；"◇"线型代表的EBDN模型的吞吐量仅次于ERMSP模型，注入攻击流量后吞吐量开始下降，最后稳定在420 Byte/s附近；"*"线型代表的SRMM模型的吞吐量指标表现较差，随着攻击流量的注入，吞吐量持续下降，最后稳定在200 Byte/s附近；"○"线型代表的是未部署ERMSP模型，随着攻击流量的注入，系统吞吐量直线下降，最后将为0，不能保证业务的连续性。因此，系统的可抵抗性由强到弱依次为：ERMSP、EBDN、SRMM和未部署ERMSP的系统。部署ERMSP模型的系统，吞吐量几乎不变，由式(2)可知，可抵抗性最强；而未部署应急响应机制的系统，吞吐量下降最快，可抵抗性最差；EBDN模型需要一定的历史数据为条件，通过机器学习机制进行决策，所以吞吐量与ERMSP模型相比略有下降。

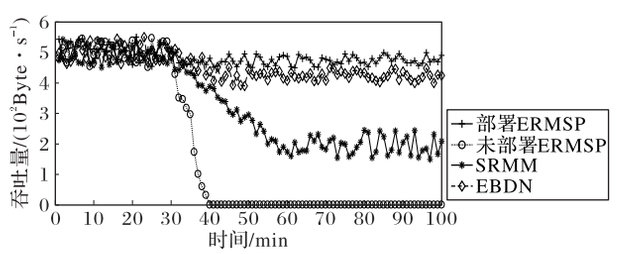

图10 SWIM可抵抗性对比

Fig. 10 Comparison of SWIM resistibility

向SWIM中注入攻击流量，测试各个服务能否正常进行，在能正常提供服务的情况下，进一步测试不同模型下系统的时延，从而在业务连续性角度判断系统应急响应能力的大小。表4是不同模型进行的业务连续性测试，实验结果表明，在注入攻击流量后，未部署应急响应机制的情况下，航空业务、航班业务和气象业务服务中断；而部署了ERMSP模型、SRMM模型和EBDN模型的系统，服务没有中断，保证了业务的连续性，但不同模型的具体表现不同，需要继续进行系统时延的测试。

表4 SWIM业务连续性测试

Tab. 4 Continuity test of SWIM business

模型服务	未部署ERMSP	部署ERMSP	SRMM	EBDN
航空业务订阅/发布	×	√	√	√
航班业务订阅/发布	×	√	√	√
气象业务订阅/发布	×	√	√	√

注：×表示异常，√表示正常。

对SWIM的时延测试结果如图11所示。图11中，统计了0~100 min四种模型下的系统平均时延，在未注入攻击流量时，四种模型的系统平均时延均为100 ms左右。在第30 min时，注入攻击流量，随着攻击流量的逐渐注入，"○"线型代表的是未部署应急响应机制的系统模型，可以看到，系统平均时延会呈指数上升，最终业务会中断，无法保证SWIM关键服务的连续性；在"*"线型代表的SRMM模型中，系统平均时延会逐渐上升，然后稳定在300 ms左右，因为每当关键服务漂移到被攻击服务器时，时延就会变大，而漂移到其他正常服务器时时延正常，因此，平均时延会增加；在"◇"线型代表的突发事件贝叶斯决策网络(EBDN)模型中，由于该模型需要大量数据和历史数据为条件，开始时网络时延会变大，后来会减小直至趋于平稳；在"+"线型代表的ERMSP模型下，当注入攻击流量后，系统监测到异常，会直接将应急消息发布到相应订阅者，及时采取应急措施，关键服务漂移到信任值较高的节点，于是时延不会有太大变化。

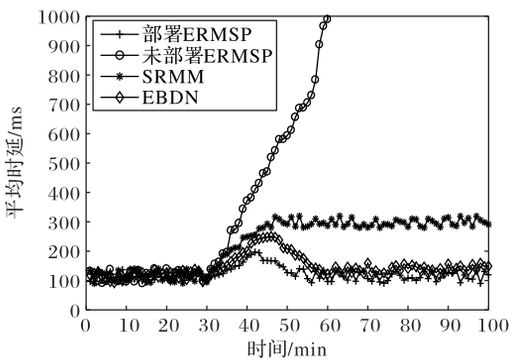

图11 不同模型下的系统平均时延

Fig. 11 Average system delay under different models

由图11可以看出，当SWIM受到攻击时，未部署应急响应机制模型下，平均时延不断上升；部署了SWMM模型时，系统稳定后，平均时延大概增加了两倍；部署了EBDN模型时，平均时延先上升后下降，之后趋于平稳，平均时延增加了20%；部署了ERMSP模型时，增加的平均时延在10%以内。

4 结语

SWIM的目标是在全球范围内实现信息的高度共享，从而提高民航系统的运行效率，因此，保证其中各个业务的连续性就显得非常重要，本文提出了基于订阅/发布服务的应急响应模型，该模型采用基于信任值的Viterbi算法进行决策，当攻击来临时，将应急消息发布到相应订阅者。仿真实验表明，该模型相对于随机服务漂移和贝叶斯决策网络模型在可识别性、可抵抗性和业务连续性等方面具有一定的优越性，能够满足SWIM应急响应的需求。本文针对SWIM应急响应系统做的工作仍需完善，在下一步工作中，从更多的角度分析此模型，进一步进行性能分析，并且考虑持续故障和间歇故障的情况。

参考文献 (References)

[1] KUN H, BO W, FENG S, et al. Design and implementation of a network emergency response mechanism based on flow and application[C]// Proceedings of the 2016 International Conference on Intelligent Transportation, Big Data and Smart City. Piscataway: IEEE, 2016:414-417.

[2] SEBA A, NOUALI-TABOUDJEMAT N, BADACHE N, et al. A review on security challenges of wireless communications in disaster emergency response and crisis management situations[J]. Journal

of Network and Computer Applications, 2019, 126:150-161.

[3] YEO J, COMFORT L, JUNG K. Timely assessment of disaster and emergency response networks in the aftermath of superstorm Sandy, 2012[J]. Online Information Review, 2018, 42(7):1010-1023.

[4] WANG X, LIN Y, ZHANG S, et al. A social activity and physical contact-based routing algorithm in mobile opportunistic networks for emergency response to sudden disasters[J]. Enterprise Information Systems, 2017, 11(5):597-626.

[5] WU Z, ZHOU S, YUE M. Research on SWIM services dynamic migration mechanism[C]// Proceedings of the IEEE 16th International Conference on Dependable, Autonomic and Secure Computing, 16th International Conference on Pervasive Intelligence and Computing, 4th International Conference on Big Data Intelligence and Computing, 3rd IEEE Cyber Science and Technology Congress. Piscataway: IEEE, 2018:1034-1039.

[6] DALAL J, ÜSTER H. Combining worst case and average case considerations in an integrated emergency response network design problem[J]. Transportation Science, 2018, 52(1):171-188.

[7] VEDULA N, PARTHASARATHY S, SHALIN V L, et al. Predicting trust relations within a social network: a case study on emergency response[C]// Proceedings of the 2017 ACM Web Science Conference. New York: ACM, 2017:53-62.

[8] QIU T, LV Y, XIA F, et al. ERGID: an efficient routing protocol for emergency response Internet of things[J]. Journal of Network and Computer Applications, 2016, 72: 104-112.

[9] ES-HAGHI M, BASTANI S. Evaluating coordination in emergency response team by using fuzzy logic through social network analysis [C]// Proceedings of the 2016 Annual Conference of the North American Fuzzy Information Processing Society. Piscataway: IEEE, 2016:1-6.

[10] QIU J, GU W, KONG Q, et al. The emergency response management based on Bayesian decision network[C]// Proceedings of the 2016 IEEE Symposium Series on Computational Intelligence. Piscataway: IEEE, 2016:1-8.

[11] GU T J, YANG W N, VILLARREAL D S. Developing an emergency response conceptual framework for network centric disaster operations[C]// Proceedings of the 3rd International Conference on Information Management. Piscataway: IEEE, 2017:252-257.

[12] LIESER P, ALVAREZ F, GARDNER-STEPHEN P, et al. Architecture for responsive emergency communications networks[C]// Proceedings of the 2017 IEEE Global Humanitarian Technology Conference. Piscataway: IEEE, 2017:1-9.

[13] 王健,赵国生. 基于SM-PEPA可生存系统认知模型及量化分析[J]. 华中科技大学学报(自然科学版), 2015, 43(5):99-103. (WANG J, ZHAO G S. Cognitive model and quantitative analysis for survivable system based on SM-PEPA[J]. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2015, 43(5):99-103.)

[14] 王鹏飞,赵文涛,张帆,等. 网络系统可生存能力量化评估的指标体系研究[J]. 计算机工程与科学, 2014, 36(6):1050-1056. (WANG P F, ZHAO W T, ZHANG F, et al. Research on index system of quantitative evaluation for network systems viability[J]. Computer Engineering and Science, 2014, 36(6):1050-1056.)

[15] 陈天平,崔文岩,孟相如,等. 性能监测下的IP网络可生存性评估方法[J]. 北京邮电大学学报, 2015, 38(6):20-23, 33. (CHEN T P, CUI W Y, MENG X R, et al. A method of IP network survivability evaluation method under performance monitoring [J]. Journal of Beijing University of Posts and Telecommunications, 2015, 38(6):20-23, 33.)

[16] KANG J, CHOI K, KIM Y, et al. A method of integrating information for SWIM[C]// Proceedings of the IEEE 13th International Symposium on Autonomous Decentralized System. Piscataway: IEEE, 2017:195-198.

[17] QI M, LU S. Overview of system wide information management and security analysis[C]// Proceedings of the IEEE 13th International Symposium on Autonomous Decentralized System. Piscataway: IEEE, 2017:191-194.

[18] ABRAHAM B. Air/ground system wide information management: concept demonstration and lessons learned[C]// Proceedings of the 2017 Integrated Communications, Navigation and Surveillance Conference. Piscataway: IEEE, 2017:2C3-1-2C3-7.

[19] MORIOKA K, LU X, KANADA N, et al. Field taxing experiments of aircraft access to SWIM over AeroMACS[C]// Proceedings of the 2018 IEEE Conference on Antenna Measurements and Applications. Piscataway: IEEE, 2018:1-4.

[20] MOALLEMI M, CARLOS-PEÑA C A, TOWHIDNEJAD M, et al. Information security in the aircraft access to system wide information management infrastructure[C]// Proceedings of the 2016 Integrated Communications, Navigation and Surveillance Conference. Piscataway: IEEE, 2016:1A3-1-1A3-7.

[21] WILSON I, YANG S. Security for system wide information management [C]// Proceedings of the 2017 Integrated Communications, Navigation and Surveillance Conference. Piscataway: IEEE, 2017:1-13.

[22] WANG Z, LUO X, ZHAO M, et al. The research of system wide information management based on SOA[C]// Proceedings of the 6th IEEE International Conference on Software Engineering and Service Science. Piscataway: IEEE, 2015:837-840.

[23] 赵汨龙,罗喜伶,王忠波. 基于SOA的民航广域信息管理架构的研究与设计[J]. 计算机技术与发展, 2016, 26(2):95-100. (ZHAO M L, LUO X L, WANG Z B. Research and design of system wide information management architecture based on SOA[J]. Computer Technology and Development, 2016, 26(2):95-100.)

[24] 袁飞飞,汪芸. 订阅/发布模式下多节点协同的数据分发方法[J]. 东南大学学报(自然科学版), 2014, 44(3):517-521. (YUAN F F, WANG Y. Data distribution method on multi-node cooperation in subscribe/publish model[J]. Journal of Southeast University (Natural Science Edition), 2014, 44(3):517-521.)

[25] International Civil Aviation Organization. ICAO SWIM concept working version v9[EB/OL]. [2019-06-20]. https://www.docin.com/p-1009906681.html.

This work is partially supported by the Joint Fund of Committee of National Natural Science Foundation of China and Civil Aviation Administration of China (U1933108), the Fundamental Research Funds for the Central Universities (3122018D34007).

WU Zhijun, born in 1965, Ph. D., professor. His research interests include network and information security.

WANG Hang, born in 1992, M. S., candidate. His research interests include system wide information management, information security.