

# 一种可信可控的网络体系及协议结构

罗军舟 韩志耕 王良民

(东南大学计算机科学与工程学院 南京 210096)

**摘 要** 互联网体系架构正面临着严峻的安全和管理挑战,迫切需要具备可信性和可控性特征的新架构.已有的网络体系结构要么是基于边缘论和面向非连接的设计思想,导致分组传输路径不可控,要么是重新设计现有网络的体系架构,代价巨大.文中提出了一种可信可控的网络体系结构,其特征是在现有网络体系架构的基础上增加一个可信可控4层逻辑结构,从而实现网络组元及用户行为的可预期、可管理,它包括决策层、观测层、资源层和可信接口层4个层次;在明确新网络体系结构中网络控制对象为逻辑流的前提下,给出了一种包含感知与监测、理解与检测、判断与决策和控制及可达4个功能环节的闭环自反馈控制方法,确保网络系统可自诊断、自恢复地回归稳定态.同时指出具备跨层交互能力的可信接口层是新体系实现可信可控的关键,继而给出了位于该层的可信可控协议模型,并定义了确保协议执行可预期的协议基本功能;指出了逻辑流中信任流是协议的主要控制对象,并基于新体系结构下网络控制方法,通过融合信任管理和不可否认服务的方式给出了协议可信的控制方法.为验证协议模型和控制方法的有效性,给出了协议的具体实施方案,包括协议基本要素和协议两阶段执行过程.最后,给出了新体系与现有技术相比较所具备的优势,并对下一步工作进行了展望.

**关键词** 可信可控;信任流;信任管理;不可否认

中图法分类号 TP393

DOI号: 10.3724/SP.J.1016.2009.00391

## Trustworthy and Controllable Network Architecture and Protocol Framework

LUO Jun-Zhou HAN Zhi-Geng WANG Liang-Min

(School of Computer Science and Engineering, Southeast University, Nanjing 210096)

**Abstract** As Internet has grown in size and complexity, the network architecture is confronting some serious challenges on security and management, and the ideal countermeasure to these issues is to design some new architecture with trustworthiness and controllability. All existing architectures are either based on End-to-End argument and connectionless-oriented theory making packets transmission uncontrollable, or redesigning the existing network architecture at great expense. With these issues in mind, the authors propose a trustworthy and controllable network architecture by attaching to the present network architecture with a four lays of trustworthy and controllable logical architecture including decision layer, observed layer, resource layer and trustworthy interaction layer for making network and user behavior predictable and manageable. On the premise of defining logic flow as the network controlled objective in the new architecture, the authors present a self-feedback control method in close-loop mode including four functional phases such as perception and monitoring, understanding and detection, judgment and decision-making, and control and reachable for ensuring network system be stable state with the capability of self-diagnosis and self-recovery. They also point out the trustworthy interaction layer with the

收稿日期:2008-07-20;最终修改稿收到日期:2009-01-14. 本课题得到国家自然科学基金(90604004,60773103)、高等学校博士学科点专项科研基金课题(200802860031)、江苏省自然科学基金重点项目(BK2007708,BK2008030)、江苏省“网络与信息安全”重点实验室项目(BM2003201)和“计算机网络和信息集成”教育部重点实验室(93K-9)资助. 罗军舟,男,1960年生,博士,教授,博士生导师,研究领域为下一代网络体系结构、协议工程、网络安全与管理、网格计算. E-mail: jl原因@seu.edu.cn. 韩志耕(通信作者),男,1976年生,博士研究生,研究方向为网络安全. E-mail: hanzgnit@seu.edu.cn. 王良民,男,1977年生,博士,研究方向为容忍入侵、安全协议.

capability of cross-layer interaction is key to ensure the network architecture trustworthy and controllable, and then propose the model of trustworthy and controllable protocol locating in the layer and define protocol fundamental function for ensuring protocol execution predictable. The authors also point out the trust flow appeared in logic flow is the protocol controlled objective, and give out protocol trustworthy control method based on network control method of the new architecture by means of integrating trust management with non-repudiation service. For checking validity of the protocol model and protocol control method, they present the concrete protocol implementing scheme including protocol basic elements and protocol two-stage execution process. Finally the authors show some advantages of our new architecture in comparison with some representative existing techniques, and point out our future work.

**Keywords** trustworthy and controllable; trust flow; trust management; non-repudiation

## 1 引 言

当今社会,互联网的基础性全局性作用不断增强,日益成为影响社会经济发展和国家安定的重要因素.然而随着网络新技术新应用的不断出现,网络规模的不断扩大,当前互联网环境已经发生了巨大变化,现有的网络体系结构日益暴露出严重的不足,主要表现在:网络系统愈加复杂异构,网络异常和攻击行为日益呈现多样性、随机性、隐蔽性和传播性,服务质量的控制和管理机制难于适应其需求的不断演化.互联网正面临着严峻的安全和管理等重大现实挑战,现有的体系结构已经不适应甚至阻碍其进一步发展,为此迫切需要提供一种新的网络体系结构来保障互联网的安全性、可信性及可控性.

从安全性角度来看,当前互联网不存在网络安全整体解决方案,虽然存在许多安全机制,但并没有一组规则能够将这些机制有效结合以实现网络的高度安全和可信.安全的体系结构必须能确保通信的高可靠和可预测、具备跨层的安全设计、合理平衡安全与隐私的矛盾.从服务质量与网络可管性角度来看,服务质量的提供从根本上依赖于对网络资源的管理和控制,互联网服务质量研究的困境源于当前互联网在体系结构上较差的可管可控性.一方面,边缘论和面向非连接的设计思想保障了高效互通,但控制手段薄弱,难以满足解决服务质量保障的需要;另一方面,作为一个庞大的非线性复杂系统,互联网“细腰模型”被打破,各种协议的决策逻辑交织在一起,使得网络行为难以预测.具备可管理和服务质量有保障的体系结构必须允许为每个网络配置针对其性能、可靠性和策略的高层需求和目标;在网络

中维护一定的状态信息,在关键部分施加必要的控制,做到在不同层次上实施监管,而将决策逻辑与分布式应用相分离<sup>①</sup>.

下一代互联网应该是可信的网络,即网络系统的行为及其结果是可以预期的,能够做到行为状态可监测、行为结果可评估、异常行为可控制;同时下一代互联网也应该是一个可管理的网络,在网络环境受到内外干扰的情况下,不但对网络状态而且对用户行为进行持续的监测、分析和决策,进而对设备、协议和机制的控制参数进行自适应优化配置,使得网络的数据传输、资源分配和用户服务的过程及结果是可以预期的<sup>[1]</sup>.为此,本文在不破坏现有网络体系结构的基础上,通过在其上增加一个可信可控的4层逻辑结构创造性地提出一种可信可控的网络体系结构,并继而给出了基于新体系结构的网络控制方法,以确保网络在满足方便管理的同时具备安全性;在此基础上进一步提出了可信可控协议模型、协议控制方法,并给出了协议的具体实施方案,包括协议基本要素和协议执行过程.新架构支撑下的网络系统通过对用户行为、网络运行状态和网络资源的有效控制和管理,实现对网络行为的可预期和可管理,即在网络受到内外干扰的情况下,对网络状态以及用户行为进行持续的检测、分析和决策,进而对设备、协议和机制等的控制参数进行自适应优化配置,使网络的数据传输、资源分配和用户服务可以达到预期的程度,从而为网络的可信可控提供必要的基础,从整体上解决当前网络的可信可控技术问题,确保向网络运行者及用户提供可信的网络服务.

① GENI: Global environment for network innovations [EB/OL]. <http://geni.net/>

## 2 相关工作

下一代互联网体系的研究是一个前瞻性课题,目前国际上还仅仅处于起步和规划阶段,并没有形成完整清晰的理论体系,所有研究工作主要从如下3个方面展开:

(1)在下一代网络体系结构方面,比较有影响的是美国自然基金委提出的 GENI(Global Environment for Networking Innovations)计划(见第2页注①)和 FIND(Future Internet Design)<sup>①</sup>计划,拟从根本上重新设计新一代信息网络,以解决现有网络在安全性、移动性、可控性、传感性和普适服务支持等方面存在的严重弊端<sup>[2]②</sup>;IETF 的 Ipng 项目组在 Ipv6 中提出了全新的网络安全体系结构 IP-Sec<sup>③</sup>,拟从协议上保证数据传输的安全性;New Arch 计划<sup>④</sup>提出了一种网络体系结构 FARA,并给出了基于现有互联网技术的实现方案 M-FARA<sup>[3]</sup>.除此之外的其它计划大多从新一代网络的某一个或几个方面展开,缺乏对新信息网络体系及关键理论的全面性、系统性研究.

(2)在网络可信性关键问题方面,值得一提的是信任机制的引入. David Clark 指出下一代网络安全体系应包括一个完善的信任机制,用于在网络实体间建立信任关系,并将信任关系转化为信任链,最终形成一个信任网络空间<sup>[4]</sup>.基于此种构想,2006年美国国家自然科学基金资助了信息空间信任(Cyber Trust)项目<sup>⑤</sup>,美国国家研究委员会也提出了信息空间信任研究建议.此外,由 Compaq 等公司牵头组织的可信计算平台组(TCG)提出了“可信计算”概念,借助信任链思想以厂商硬件为信任根,层层往上信任,建立可信计算环境.然而以上研究都将重点放在信任机制本身,缺乏对信任机制所依赖的控制机制进行研究.

(3)在网络控制体系及关键问题方面,比较有影响的是 CMU 牵头提出的“网络控制与管理的4D 结构”<sup>⑥</sup>和 GENI 计划支持的研究.4D 结构对现有网络体系进行了改进,在此基础上文献[5]进一步提出了4D网络控制架构,将网络控制的4个环节映射成4个层面:决策层、发现层、数据层和分层,重点将决策层与数据层相剥离,强调决策层的独立性,以建立一个完整的网络管理逻辑视图,从而提高网络管理和控制能力;CONMan 在4D基础上进一步强调了控制管理与数据转发两种功能的分离<sup>[6]</sup>.

虽然4D网络控制架构可以带来更快的响应时间、更小的开销和更大的可用性<sup>[2,7-8]</sup>,但未能考虑到相关层面间的协同决策与最优控制问题. GENI 计划在试验床设计规范的管理部份提出了将数据转发等元管理(Meta-Management)功能与其它高级控制功能进行逻辑分离,将元管理功能以一种服务接口形式提供给高层的控制平台,而将控制平台与具体网元设备相剥离<sup>[9-10]</sup>.需要说明的是,GENI 计划中有关网络控制方法还处于试验床设计阶段,而对网络控制模型中的网络要素相关性、协议可信性验证以及网络管理逻辑视图建立等具体理论问题还没有完整的概念.

我国在下一代网络体系结构、可信性和可控性方面有着多年的研究;清华大学、东南大学、北京交通大学和北京邮电大学等国内知名院校在新一代互联网体系、高可用网络体系结构、可信可控网络、一体化可信网络、可测可控可管的IP网领域进行了不少前瞻性的研究.东南大学顾冠群院士创建的计算机网络与通信研究室,明确指出了下一代网络具有网络本身、网络服务和网络应用3个层次特性,从OSI体系结构到高速网络和高性能网络的体系结构的研究,取得了一系列成果.以高可用网络为目标,这个团队提出了基于交互的网络服务体系结构(INSAs),通过结构分层、功能分面、基于交互、面向服务的原则设计网络体系,并对体系中各功能组件进行了具体定义和形式化建模<sup>[11]</sup>.清华大学吴建平教授2003年开始承担的国家“九七三”计划项目“新一代互联网体系结构理论研究”,围绕新一代互联网体系结构理论研究中存在的若干关键的科学问题,在多维可扩展的互联网体系结构模型和协议理论、新一代互联网路由与交换理论、互联网的突发流量行为基础理论、互联网动态自适应传输控制理论、可信互联网安全体系结构和安全监控理论和互联网服务模型及其管理理论等方面展开研究,取得了一系列创新性成果,提出了新一代互联网体系结构包

- ① FIND: Future Internet design [EB/OL]. <http://find.isi.edu/>
- ② Peterson L, Anderson T, Blumenthal D et al. GENI design principles [EB/OL]. <http://geni.net/GDD/GDD-06-08.pdf>
- ③ Friedl. An illustrated guide to IPsec [EB/OL]. <http://www.unixwiz.net/techtips/iguide-ipsec.html>
- ④ NewArch project: Future-generation Internet architecture [EB/OL]. <http://www.isi.edu/newarch/>
- ⑤ Cyber Trust [EB/OL]. <http://www.nap.edu/catalog/6161.html>
- ⑥ The 4D Architecture for Network Control and Management [EB/OL]. <http://www.cs.cmu.edu/~4D/>

含的 5 个基本要素和构建“基于 IPv6 真实地址的可信任新一代互联网”的重大学术思想<sup>[12]</sup>. 清华大学林闯教授基于 4D 网络控制架构提出了可信可控网的概念,认为通过 4D 架构能够达到一个可信、可控、可扩展的网络,但必须解决其控制的可信性. 在可信可控网络体系的研究,林闯教授团队认为要建立一个完整的可信网络,必须解决如下问题:网络与用户行为的可信模型、可信的网络体系、服务的可生存性以及网络的可管理性<sup>[1]</sup>. 北京交通大学张宏科教授主持的国家“九七三”计划项目“一体化可信网络与普适服务体系基础研究”,瞄准了下一代信息网络的需求,力求创建一体化可信网络,攻克新一代信息网络及其重大应用的基础性技术. 他们进行了一体化网络与普适服务体系理论研究,试图解决在一体化网络与普适服务体系下的可信理论问题,将网络体系分为“网通层”和“服务层”两个层面,“网通层”完成网络一体化,服务层实现服务普适化,这两层模型结合在一起,构成了一体化网络与普适服务体系的基础理论框架<sup>[13]</sup>. 北京邮电大学孟洛明教授主持的国家“九七三”计划项目“可测可控可管的 IP 网的基础研究”,已经开始了 IP 网络可管理方面的研究<sup>[14]</sup>.

3 可信可控网络体系

我们认为未来互联网体系结构必须至少做到两点:(1)从用户角度来讲需要确保网络的可信性,从体系结构设计角度来讲需要确保网络的可控性;(2)可信性和可控性能在体系结构框架内做到很好地融合. 要实现上述两点,网络可信控制必须得到有效解决.

目前围绕网络可信控制问题还没有形成一个完整清晰的认识,可信的网络控制方法尚在探讨,尚没有一个网络控制模型或一套控制方法满足 GENI 计划所认为的可信的下一代网络控制系统应具备的 3 个特征:可靠的系统信息来源、可信的决策诊断机制和自适应的系统控制方法,即控制系统应为设备提供上报错误信息的可靠通道;系统应提供一个完整的诊断工具,为管理行为进行有意义的信息反馈;系统可根据网络运营者的高层策略定义及系统诊断结论,自适应重构或重配置系统组元,这就是所谓的可观、可控、可达 3 种属性. 基于此,本节提出一种可信可控网络体系,并给出该体系支撑下的网络控制方法.

3.1 可信可控 4 层逻辑结构

本文给出一种可信可控的网络体系结构(如

图 1 所示),其特征是不破坏现有的 OSI 七层体系结构以及 TCP/IP 四层体系结构来重建一个新的网络体系结构,而是在此基础上增加一个可信可控 4 层逻辑结构,从而实现网络组元及用户行为的可预期、可管理. 它包括“决策层”、“观测层”、“资源层”和“可信接口层”4 个层次;其中“可信接口层”以协议跨层的方式实现现有网络体系与资源层的交互;“资源层”通过可信接口层的协议为观测层提供“资源流”;“观测层”从包含资源流和“信任流”的“逻辑流”中提取特征,为决策层提供一个具有较好一致性 & 可观性的视图;“决策层”根据可观视图,从系统当前态势及全局利益最大化角度出发提出控制方案,通过接口层提供给网络,达到控制的目的,同时给出该时刻各组元的信度,以信任流的形式通过可信接口层提供给观测层. 该架构支撑下的网络系统的可控性特征在于以监控、检测、分析、决策、控制等多个环节而自适应地形成一个自反馈的控制系统,以闭环方式实现网络系统的完全可控性.

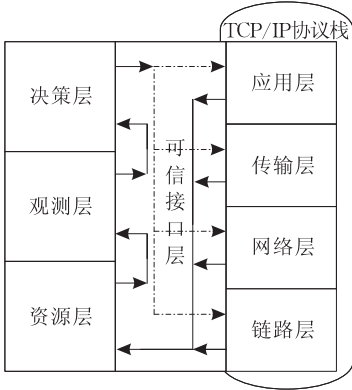


图 1 可信可控网络体系结构图

具体来讲:

“资源层”对网络运行期间的各种状态进行及时感知,将感知和监测的结果转化为基于时间序列的资源流,并通过接口层提交给观测层. 该资源流的特征为除了包含网络状态,如数据传输及资源分配等的时序变化,也包含基于时间序列的用户行为信息.

“观测层”给决策层提供具有一致性和可观性的逻辑流视图,目的是对故障、攻击和服务质量下降等异常现象及用户异常行为进行及时检测和识别,其特征是从由资源流和信任流组成的“逻辑流”中抽取异常信息,来判断或识别出异常及变化情况. 具体手段是汇聚来自资源层的网元资源流以及来自决策层关于网元历史行为而赋予的信度值,形成具有一致性的逻辑流,并从逻辑流抽取特征,根据特征检测或识别出异常及变化情况,以某种可观的简明形式由

接口层转发给决策层。

“决策层”是控制命令的形成阶段，其特征是根据观测的结果，采用基于博弈、表决、协同、竞争等多种手段，结合系统当前态势，给出控制的措施，该措施实施的特征为对抽象的逻辑流进行更新，并将更新通过接口层提交给网络系统。

“可信接口层”扮演着重要的跨层交互角色，其特征是以跨层交互的共享平台模式，沟通了决策、观测及资源 3 个抽象的逻辑层面，同时完成了资源层及决策层与网络系统的交互。该交互涉及到原有网络系统的多个层面，可信接口层成为基本的管理各种网络资源不可或缺的统一平台，使得任何协议、转发技术都可以在这个平台上共存，完成与新的可信可控体系的交互。

可信可控 4 层逻辑结构中各层间交互的基本元素是逻辑流，该逻辑流的基本特征是以具有一致性模式的基于时序的信息流体现网络参数及服务运行情况，该信息流包括通过接口层协议获得基于时序的用户行为、网络状态及网络资源以及各网络组元的信度变化情况，信任流是该逻辑流的不可或缺的组成部分。信任流是基于时序的网元信度变化序列，其特征是决策层根据网元历史行为而赋予其一定的信度值，该信度值可以反映服务及资源的运行情况、入侵情况。

系统运行过程中可能经过多个状态，基于可信可控网络体系结构的控制的目的是使得整个网络系统在运行期内以闭环自反馈方式运行，如图 2 所示，网络系统由最初的稳定态经过中间状态(系统扰动产生的多个中间状态)后，进入控制态(系统控制过程产生的多个中间状态)，最终回到稳定态，形成一个闭环的控制系统。

制论的思想和方法，用统一、综合、科学、系统的观点和分析方法，研究网络系统运动的运动变化过程及其相互关系，揭示网络系统在安全、管理、反馈和稳定性等一系列特性方面的内在联系，目的在于提供运行状态好、稳定、可靠、协调的网络系统及网络技术。可信可控网络体系下的网络控制对象为逻辑流，整个过程由感知与监测、理解与检测、判断与决策和控制及可达 4 个功能环节协作完成(如图 2)。

具体控制过程如下：

(1)感知与监测环节监测到网络系统受外界扰动发生的变化后，将网络状态(如数据传输、资源分配)及用户行为等变化以基于时间序列资源流的形式提供给理解与检测环节。

(2)理解与检测环节根据来自感知与监测环节的资源信息进行故障分析以及来自判断与决策环节根据组元历史行为给出的信度，进行理解与分析，对有疑虑问题，进行检测分析、服务质量分析等，从而给整个网络状态及服务情况提供一个可观视图给判断与决策环节。

(3)判断与决策环节根据来自理解与检测环节的可观视图，进行一致性分析，这些分析包括信任重估、态势评估、系统预警、组元表决、联盟博弈等，判断与决策环节根据这些基于整体的分析，采取具体控制措施，以逻辑流中控制流的形式传播给控制及可达环节。

(4)控制及可达环节负责执行控制命令，不仅包括资源重组、系统重构、组元隔离，还包括对系统执行情况的反馈。

(5)控制与扰动一起，对系统进行调整，其最终目的是使得系统回归稳定态，整个控制过程以闭环形式自适应运行。

4 可信可控协议

可信接口层作为确保该新架构可信可控的关键，以跨层交互的共享平台模式确保能在统一的网络级目标下，建立网络状态信息的共享决策模式。具体来讲包括 3 个方面：(1)将各协议层次的网络状态发布到相关协议层；(2)将状态分析逻辑的相关信息由本层扩展到相关层；(3)将各层独立实施的网路控制变为多层间动态自适应的关联控制。可信接口层在逻辑上包含一组“可信可控协议”，为网络状态信息共享决策模式的实现在网络组元间提供安全可预期的信息交互。

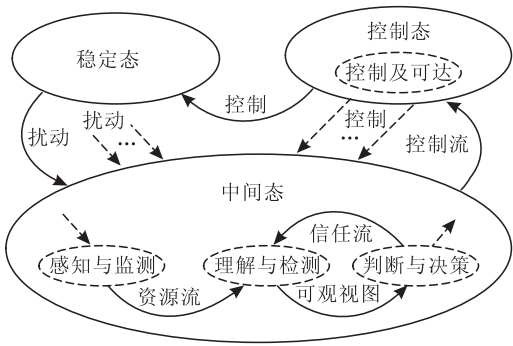


图 2 网络系统状态迁移图

3.2 基于可信可控网络体系的网络控制方法

所谓网络控制<sup>[15]</sup>，就是针对充满不定性、关联性并不断发展的网络系统，遵循信息论、系统论和控



4.1 可信可控协议模型

根据可信可控网络体系结构,信任流是可信接口层管理的对象,新体系架构能够得到正确实施的关键之一是可信接口层可对信任流实施有效的管理控制. 基于此,受网络控制论思想的启发<sup>[15]</sup>,给出如图 3 和图 4 所示的具有闭环自反馈特征的可信可控协议模型. 通过对信任流实施具备可观性、可控性和可达性等特征的自反馈控制,以此来最终确保协议执行的可信赖、可预期.

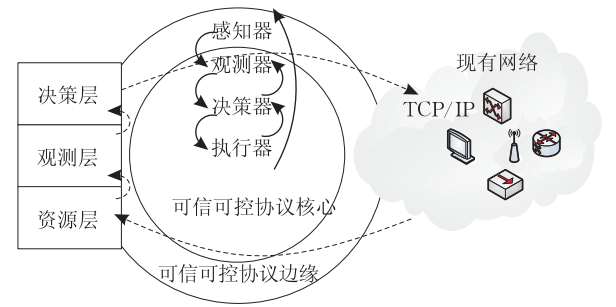


图 3 控制过程角度

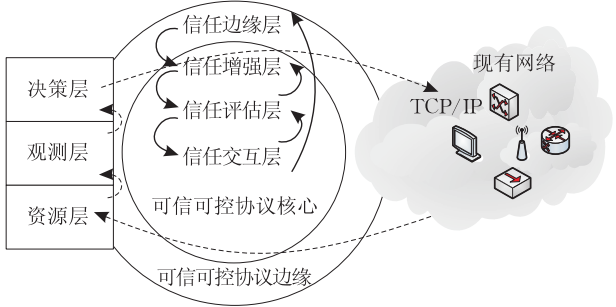


图 4 信任管理角度

从控制过程角度来讲(见图 3),为了保证协议执行的可信可控,需要实现 3 个方面的条件,即处于协议边缘的感知器能够准确反映信任度的变化,信任度的变化在协议核心处的观测器、决策器和执行器所能控制的范围内,协作网络能够保证信任流在相应组元间的流动,这就是所谓的可观、可控及可达 3 种属性.

从信任管理角度来讲(见图 4),为了保证协议执行的可信可控,处于协议边缘的信任边缘层能够从协议交互中拥有信任变化态势;处于协议核心处的信任增强层能够有效改善协议交互中网络组元的信任度,信任评估层能够对协议交互过程和结果作出准确评估,信任交互层能够确保信任信息在网络组元间有效共享.

需要说明的是,可信可控协议仅是一种逻辑意义上的协议,不是物理意义上的网络协议. 可信可控协议构建于现有网络协议之上,不会试图破坏原有

网络协议是同层实体间交互规约的基本点. 这样构建的用意在于,传统的网络协议仅为网络中对等实体间的信息交互提供规范,并没有考虑在网络系统脆弱性不可避免以及攻击或破坏行为客观存在情况下对交互行为实施控制的问题,难以保证协议执行的安全可信性. 可信可控协议模型主要用于实现恶意行为存在时的协议交互控制问题,确保任何一组“行为良好”的网络组元之间能够任意进行安全可预期的信息交互,而使恶意或遭到破坏的网络组元无法干预这种交互.

4.2 可信可控协议功能

可信可控协议应该是参与协议的实体行为及协议执行结果是可预期的,能够做到协议实体行为可度量、协议执行状态可监测、协议执行结果可评估、协议执行事后可追究、协议异常执行可控制. 具体而言,从协议用户的角度需要保障协议的可信性:一方面,当协议所提供的服务安全时,其对用户来说是完全可以信任的;另一方面,当协议所提供的服务不安全时,享有该服务所存在的风险应是用户可以承担的. 从设计角度则需提供协议的可控性. 不同于可信性、可控性在传统意义上分散、孤立的概念内涵,可信可控协议将在网络框架内融合可信性和可控性,围绕协议实体间信任的维护和行为控制形成一个有机整体. 受文献<sup>[16]</sup>启发,给出图 5 所示的可信可控协议核心框架.

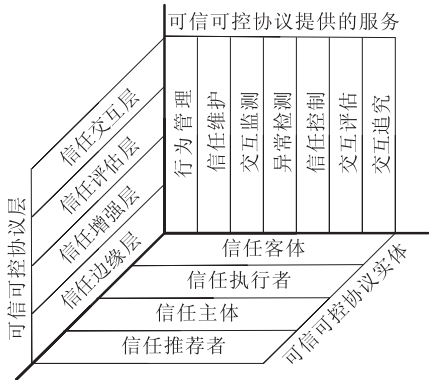


图 5 可信可控协议核心框架

可信可控协议研究思路如图 6 所示. 可信可控协议主要目标是确保协议执行可预期. 满足该目标的协议必须具备 3 个主要特征:可靠的信任信息来源、实时动态的信任分析决策机制和可控的协议执行方法. 为此,协议必须能够实现 4 个基本功能:一方面,可靠的信任信息来源和实时动态的信任分析决策机制要求协议能够实现实体行为的可观性、信任模型的鲁棒性和信任信息的可达性;另一方面,可

控的协议执行方法要求协议能实现执行的可控性。

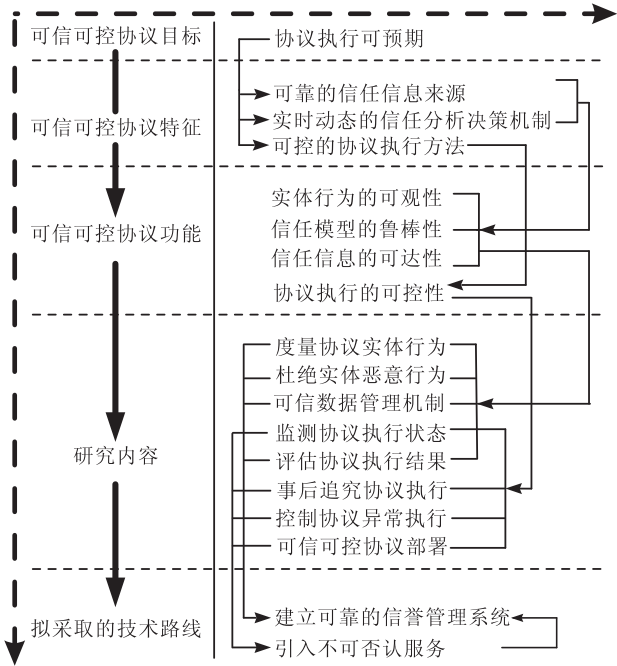


图 6 可信可控协议研究思路

实现上述 4 个功能需要给出相应的算法与机制，我们认为需要从 8 点展开：(1) 度量协议实体行

为；(2) 杜绝协议实体恶意行为；(3) 信任数据管理机制；(4) 监测协议执行状态；(5) 评估协议执行结果；(6) 事后追究协议执行；(7) 控制协议异常执行；(8) 可信可控协议安全部署。其中(1)(2)(3)(5)用于确保实体行为的可观性、信任模型的鲁棒性和信任信息的可达性，(4)(6)(7)(8)用于确保协议执行的可控性。

拟采取的技术路线为：(1)(2)(3)(5)归结为建立一种可靠的信任/信誉管理系统<sup>[17-19]</sup>；(4)(6)(7)(8)通过引入不可否认服务<sup>[20-24]</sup>来实现；同时信任/信誉管理系统可靠性的获得也需要得到不可否认服务的支持<sup>[17]</sup>。

### 5 可信可控协议控制方法

可信可控网络体系支撑下的遵循网络可信控制方法的协议可信控制过程由感知器(实现感知与监测环节)、观测器(实现理解与检测环节)、决策器(实现判断与决策环节)和执行器(实现控制及可达环节)4 个逻辑功能部件协作完成，如图 7 所示。

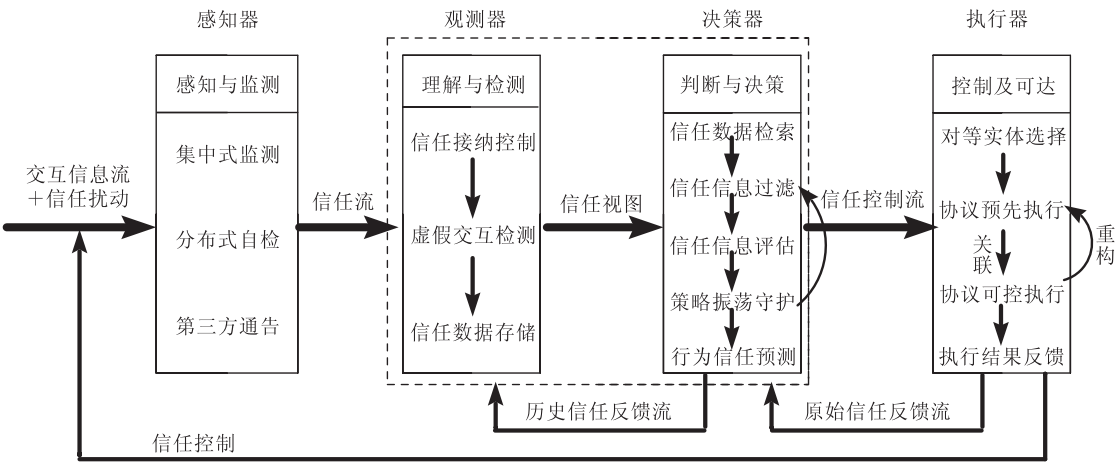


图 7 可信可控协议控制过程

鉴于网络控制论系统是由离散事件驱动，并由离散事件按照一定运行规则相互作用，来导致状态演化的一类动态系统，故考虑在协议可信控制过程的描述中，采用图 8 所示信任流时序图，向量 $\langle \dots, flow_{i-1}, flow_i, flow_{i+1}, \dots \rangle$ 标识信任流，其中分量 $flow_i$ 用于标识第  $i$  个时间区域内网络系统的整体信任态势。 $flow_i$ 长短反映了控制系统对网络系统中信任态势变化的敏感粒度，由感知器、观测器、决策器和执行器 4 个功能部件单位时间内的处理能力共

同决定。此外  $y=x-1$ ,  $x+1$ ,  $x-4$  分别标识  $y$  为当前时间区域  $x$  的上一个、下一个、之前的第 4 个时间区域。可信可控协议系统的控制过程描述如下：

(1) 感知器对来自现有网络与可信可控跨层架构组元(资源层、观测层和决策层)间带信任扰动的交互流(逻辑流)变化态势进行感知与监测，从中抽取观测器能够理解和检测的信任流。感知和监测的方式可以为集中式监测、分布式自检或第三方通告等。如下式：

$$\begin{pmatrix} LFwTD_{r_1 t_1} & \cdots & LFwTD_{r_1 t} \\ \vdots & \ddots & \vdots \\ LFwTD_{r_m t_1} & \cdots & LFwTD_{r_m t} \end{pmatrix}_{m \times (t-t_1+1)} \triangleq \begin{pmatrix} TF_{r_a t_1} & \cdots & TF_{r_a t} \\ \vdots & \ddots & \vdots \\ TF_{r_b t_1} & \cdots & TF_{r_b t} \end{pmatrix}_{n \times (t-t_1+1)} \quad (1)$$

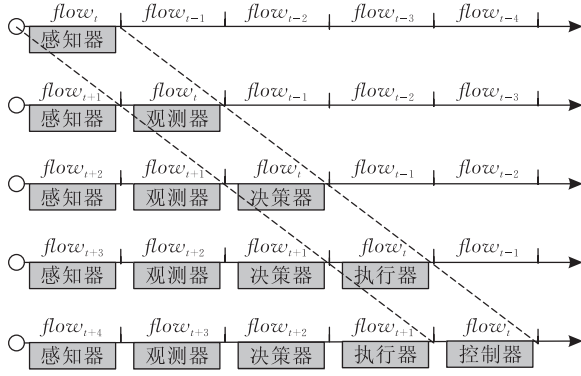


图 8 信任流处理时序图

式(1)左侧为  $m$  个  $(t-t_1+1)$  维行向量组成的交互矩阵,用于标识协议系统所能感知到的带扰动信息的交互流在时间区域  $[t_1, t]$  内的变化态势;右侧为  $n$  个  $(t-t_1+1)$  维行向量组成的待提交给观测器的信任流矩阵,用于标识网络系统中信任变化态势;  $[\phi_0](\cdot)$  为感知与监测变换,完成从交互信息流到信任流的映射;由于信任流是交互流(逻辑流)的一部分,此处有  $n < m$ 。

(2) 观测器对来自感知器输出的原始信任流以及决策器反馈的历史信任流进行理解和检测,并将处理结果以信任视图的方式提供给决策器进行判断与决策。具体来讲:观测器依据信任接纳控制机制对感知器提供的原始信任流以及决策器反馈的历史信任流进行处理,从其中剔除掉虚假信任交互产生的“信任数据”,并借助于信任数据存储服务将信任数据安全地储存到相关节点保存,从而可为决策器提供一个可观的信任视图。如下式

$$\begin{pmatrix} TF_{r_a t_1} & \cdots & TF_{r_a t} \\ \vdots & \ddots & \vdots \\ TF_{r_b t_1} & \cdots & TF_{r_b t} \end{pmatrix}_{n \times (t-t_1+1)} \oplus_0 \begin{pmatrix} HTF_{r_c t_1}^2 & \cdots & HTF_{r_c t}^2 \\ \vdots & \ddots & \vdots \\ HTF_{r_d t_1}^2 & \cdots & HTF_{r_d t}^2 \end{pmatrix}_{p \times (t-t_1+1)} \triangleq \begin{pmatrix} TV_{r_e t_1} & \cdots & TV_{r_e t} \\ \vdots & \ddots & \vdots \\ TV_{r_f t_1} & \cdots & TV_{r_f t} \end{pmatrix}_{q \times (t-t_1+1)} \quad (2)$$

式(2)中有  $t' = t-1$ ,  $t'_1 = t_1-1$ ,  $n \times (t-t_1+1)$  维矩阵标识感知器提交的信任流,  $p \times (t-t_1+1)$  维矩阵标识决策器反馈的历史信任流,  $\oplus_0$  运算整合原始信任流和历史信任流,  $[\lambda_0]$  标识历史信任流的整合权重,  $q \times (t-t_1+1)$  维矩阵标识待提交给决策器的信任视图,  $[\phi_1](\cdot)$  为理解与检测变换,用于完成从信任流到信任视图的映射。

(3) 决策器对来自观测器的信任视图和执行器的原始反馈信任流进行判断与决策,并将结果按两种形式进行处理: (1') 以信任控制流形式提供给执行器进行控制及可达处理; (2') 以历史信任流形式反馈给观测器进行理解与检测。具体来讲:决策器从观测器提供的信任视图以及执行器提供的原始反馈信任流中检索出相关的信任数据,经过策略振荡守护和信任信息过滤处理后利用信任评估引擎进行信任评估(计算出信任值),当评估结果满足预设要求(如信任值不低于信任阈值)时,再依据一定的策略进行行为信任预测,处理结果要么以信任控制流形式提供给执行器,要么以历史信任流形式反馈给观测器。如下式

$$\begin{pmatrix} TV_{r_e t_1} & \cdots & TV_{r_e t} \\ \vdots & \ddots & \vdots \\ TV_{r_f t_1} & \cdots & TV_{r_f t} \end{pmatrix}_{q \times (t-t_1+1)} \oplus_1 \begin{pmatrix} RTF_{r_g t_1}^2 & \cdots & RTF_{r_g t}^2 \\ \vdots & \ddots & \vdots \\ RTF_{r_h t_1}^2 & \cdots & RTF_{r_h t}^2 \end{pmatrix}_{s \times (t-t_1+1)} \triangleq \begin{pmatrix} HTF_{r_i t_1}^2 & \cdots & HTF_{r_i t}^2 \\ \vdots & \ddots & \vdots \\ HTF_{r_j t_1}^2 & \cdots & HTF_{r_j t}^2 \end{pmatrix}_{u \times (t-t_1+1)} \oplus_2 \begin{pmatrix} TCF_{r_k t_1} & \cdots & TCF_{r_k t} \\ \vdots & \ddots & \vdots \\ TCF_{r_l t_1} & \cdots & TCF_{r_l t} \end{pmatrix}_{v \times (t-t_1+1)} \quad (3)$$

式(3)中有  $t' = t-1$ ,  $t'_1 = t_1-1$ ,  $q \times (t-t_1+1)$  维矩阵标识观测器提交的信任视图,  $s \times (t-t_1+1)$  维矩阵标识执行器提供的原始历史反馈信任流,  $\oplus_1$  运算整合信任视图和原始历史反馈信任流,  $[\lambda_1]$  标识原始历史反馈信任流的整合权重,  $u \times (t-t_1+1)$  维矩阵标识待提交给观测器的历史信任流,  $v \times (t-t_1+1)$  维矩阵标识待提交给执行器的信任控制流,  $[\phi_2](\cdot)$  和  $[\phi_3](\cdot)$  为判断与决策变换,完成整合后的信任视图和原始历史反馈信任流到信任控制流和历史反馈信任流的映射,  $\oplus_2$  执行流分解运算。



(4) 执行器对决策器提交的信任控制流进行控制及可达处理, 并将执行结果按两种形式进行处理: (1') 以信任控制命令形式作用于带扰动的交互信息流; (2') 将信任数据以原始信任流形式反馈给决策器进行判断与决策. 具体来讲: 执行器解析决策器提供的信任控制流, 继而启用信任节点选择服务进行对等实体选择(输出为对等实体集). 协议执行分为两个阶段: 协议预先执行和协议可控执行. 在预先执行阶段, 执行器主要任务是在不可否认框架内, 采用特定算法派生出可关联本次协议轮的“交互证据”, 并在对等实体集内交换它们. 该阶段的主要目的是确保协议执行事后可追究. 在协议可控执行阶段, 对等实体集内元素间执行具体的协议交互, 执行器采用一定的机制对协议执行状态进行监测, 并依据相关策略对执行异常进行控制. 执行器将最终结果分类处理, 一类是用于控制目的控制命令, 一类是待反馈给决策器的原始反馈信任流. 如下式

$$\begin{aligned} & \begin{bmatrix} TCF_{r_k t_1} & \cdots & TCF_{r_k t} \\ \vdots & \ddots & \vdots \\ TCF_{r_l t_1} & \cdots & TCF_{r_l t} \end{bmatrix}_{v \times (t-t_1+1)} \triangleq \\ & [\phi_4]_{v \times w} \begin{bmatrix} RTF^2_{r_k t_1} & \cdots & RTF^2_{r_k t} \\ \vdots & \ddots & \vdots \\ RTF^2_{r_h t_1} & \cdots & RTF^2_{r_h t} \end{bmatrix}_{w \times (t-t_1+1)} \oplus_3 \\ & [\phi_5]_{v \times x} \begin{bmatrix} \langle TCC_{r_i t} \rangle \\ \vdots \\ \langle TCC_{r_j t} \rangle \end{bmatrix}_{x \times 1} [\phi_6]_{1 \times (t-t_1+1)} \quad (4) \end{aligned}$$

式(4)中  $v \times (t-t_1+1)$  维矩阵标识决策器提交的信任控制流,  $w \times (t-t_1+1)$  维矩阵标识待提交给决策器的原始历史反馈信任流,  $x \times 1$  维矩阵标识信任控制命令集, 每个行向量为一个信任控制命令子序列;  $[\phi_4](\cdot)$  和  $[\phi_5](\cdot)[\phi_6]$  为控制及可达变换, 分别完成从信任控制流到待提交给决策器的原始历史反馈信任流和待作用于交互信息流(逻辑流)的控制命令集的映射.  $\oplus_3$  执行信任流与信任控制命令的分解运算.

(5) 信任控制与信任扰动一起, 对系统中信任

数据进行动态调整, 其最终目的是使得网络系统中信任态势随着协议交互回归稳定, 整个信任控制过程以闭环反馈形式自适应地运行. 如下式

$$\begin{aligned} & \lim_{x \rightarrow T} \left[ \begin{bmatrix} LFwTD_{r_1 t_1} & \cdots & LFwTD_{r_1 t} \\ \vdots & \ddots & \vdots \\ LFwTD_{r_m t_1} & \cdots & LFwTD_{r_m t} \end{bmatrix}_{m \times (t-t_1+1)} \oplus_4 \right. \\ & \left. [\lambda_2]_{m \times y} \begin{bmatrix} \langle TCC_{r_k t^*} \rangle \\ \vdots \\ \langle TCC_{r_l t^*} \rangle \end{bmatrix}_{y \times 1} [\lambda_3]_{1 \times (t-t_1+1)} \right] \ominus_0 \\ & \left[ \begin{bmatrix} LFwTD_{r_1 t'_1} & \cdots & LFwTD_{r_1 t'} \\ \vdots & \ddots & \vdots \\ LFwTD_{r_m t'_1} & \cdots & LFwTD_{r_m t'} \end{bmatrix}_{m \times (t-t_1+1)} \oplus_4 \right. \\ & \left. [\lambda_{14}]_{m \times z} \begin{bmatrix} FC_{r_u t'^*} \\ \vdots \\ FC_{r_v t'^*} \end{bmatrix}_{z \times 1} [\lambda_5]_{1 \times (t-t_1+1)} \right] \triangleleft \\ & [\xi_{ij}]_{m \times (t-t_1+1)} \quad (5) \end{aligned}$$

式(5)中有  $t^* = t-4$ ,  $t'^* = t'-4$ ,  $t' = t-1$ ,  $t'_1 = t_1-1$ , 运算  $\oplus_4$  用于对交互信息流实施控制,  $[\lambda_2](\cdot)[\lambda_3]$  和  $[\lambda_4](\cdot)[\lambda_5]$  为信任控制命令作用的力度; 运算  $\ominus_0$  用于量化判断两个时间区域内交互信息流的变化幅度;  $T$  定义了系统从最初信任稳定态, 经过若干信任中间态和信任控制态再次回到信任稳定态所耗费的时间, 其中  $x$  标识时间区域  $[t_1, t]$  的长度;  $[\xi_{ij}]$  为系统定义的信任变化阈值, 若相邻时间区域内信息流变化幅度小于该阈值, 则视系统处于信任稳定态.

## 6 可信可控协议实施方法

在可信可控协议模型、协议功能和控制方法的基础上, 通过引入可靠信任/信誉管理和不可否认服务对文献[16]的理论成果进行扩充, 给出可信可控协议逻辑意义上的实施方法, 包括协议基本要素和协议执行过程.

### 6.1 协议基本要素

可信可控协议基本要素包括协议逻辑功能实体和协议逻辑功能组件(见表1).

表 1 可信可控协议基本要素

	信任边缘层	信任增强层	信任评估层	信任交互层
信任客体	行为请求点(BRP) 纠纷引发点(DTP)	增强请求点(ERP)	信任度量代理(TMA)	信任交互客户方(TEC)
信任执行者	信任执行点(TExP) 纠纷处理点(DDP)	交互检测点(EDP)	信任过滤点(TFiP)	信任反馈点(TFeP)
信任主体	行为授权点(BAP) 纠纷受理点(DAP)	增强服务点(ESP) 信任数据访问点(TDAP)	信任评估点(TEvP) 信任预测点(TPP)	信任交互服务方(TES) 纠纷解决点(DRP)
信任推荐者	行为授权点(BAP)		信任推荐点(TRP)	信任推荐服务方(TRS)

首先,给出 4 个逻辑功能实体,包括信任客体、信任执行者、信任主体和信任推荐者:

(1)信任客体是指为了参与协议交互而需要得到信任主体信任的实体,可以是参与交互的网络组元以及网络用户,信任重点应放在实体标识、实体状态以及实体交互行为上.

(2)信任执行者是指依据信任主体制定的策略执行信任交互控制的实体,可以是执行交互控制的物理单元,也可以是一组相关的算法与机制.

(3)信任主体是指依据信任客体的交互行为执行信任管理以及授权信任执行者执行信任控制的实体.

(4)信任推荐者是特殊类型的信任主体,能够依据所拥有的行为信任记录,通过信任推荐的方式辅助信任主体完成对信任客体的信任管理.

其次,给出协议逻辑功能组件,包括信任边缘层协议组件、信任增强层协议组件、信任评估层协议组件和信任交互层协议组件:

(1)信任边缘层协议组件

行为请求点(Behavior Requirement Point, BRP)运行在信任客体上,用于向信任执行点(Trustworthiness Execution Point, TExP)提出行为请求.纠纷引发点(Dispute Trigger Point, DTP)作为 BRP 的功能子单元,当信任客体对交互有异议时,通过其向纠纷处理点(Dispute Disposal Point, DDP)提出纠纷处理请求. TExP 运行在信任执行者上,依据行为授权点(Behavior Authorization Point, BAP)赋予的控制指令对信任客体进行控制. DDP 作为信任执行点的功能子单元运行在信任执行者处,负责接收纠纷处理请求,并依据纠纷受理点(Dispute Accept Point, DAP)提供的策略解决纠纷.行为授权点(Behavior Authorization Point, BAP)运行在信任主体上,将信任执行点提交的控制请求转发给信任交互服务方,并将最终信任控制策略反馈给 TExP;此外,信任推荐者通过 BAP 将与控制请求相关的已有信任控制策略推荐给信任主体. DAP 作为 BAP 的功能子单元,负责归类、分析和转发纠纷处理请求给纠纷解决点,并将纠纷解决策略反馈给 DDP.

(2)信任增强层协议组件

增强请求点(Enhancement Require Point, ERP)运行在信任客体处,根据信任评估点提供的评

估结果请求运行在信任主体处的增强服务点(Enhancement Sever Point, ESP)提供相应的策略来改善信任客体的信誉值.交互检测点(Exchange Detection Point, EDP)运行在信任执行者处,负责提供可信数据入库前的接纳控制服务,检测出虚假交互所产生的伪信任数据.信任数据访问点(Trust Data Access Point, TDAP)运行在信任主体处,负责使用相应的资源定位机制提供可信可控的数据访问服务.

(3)信任评估层协议组件

信任度量代理(Trustworthiness Measure Agent, TMA)运行在信任客体处,负责收集评估证据,并将其提交给信任评估点(Trustworthiness Evaluation Point, TEvP).信任过滤点(Trustworthiness Filter Point, TFiP)运行在信任执行者处,负责对数据进行信任过滤,剔除来自策略振荡实体的数据,从而确保信任数据的一致性. TEvP 运行在信任主体处,利用信任评估算法进行信任评估.信任预测点(Trustworthiness Prediction Point, TPP)同样运行在信任主体处,根据信任客体的已有行为上下文预测其未来行为趋势.信任推荐点(Trustworthiness Recommendation Point, TRP)运行在信任推荐者处,拥有与信任客体相关的某些信任评估证据,并在必要的时候作出推荐.

(4)信任交互层协议组件

信任交互客户方(Trustworthiness Exchange Client, TEC)、信任反馈点(Trustworthiness Feedback Point, TFeP)、信任交互服务方(Trustworthiness Exchange Server, TES)、纠纷解决点(Dispute Resolution Point, DRP)、信任推荐服务方(Trustworthiness Recommendation Server, TRS)之间存在一个安全信道,通过其 TEvP 能够获取来自信任度量代理和信任推荐点所提交的信任评估证据. TFeP 运行在信任执行者处,通过分析协议交互结果,从而提交相应的建议给信任交互服务方作为决策未来协议执行的必要依据. DRP 作为 TES 的功能子单元运行在信任主体处,负责接收来自 DAP 的纠纷解决请求,并制定出纠纷解决策略.

6.2 协议执行

根据可信可控协议模型和协议控制方法,新体系支撑下的可信可控协议逻辑执行框架包括信任控制和纠纷处理两部分,步骤描述如下(见图 9).

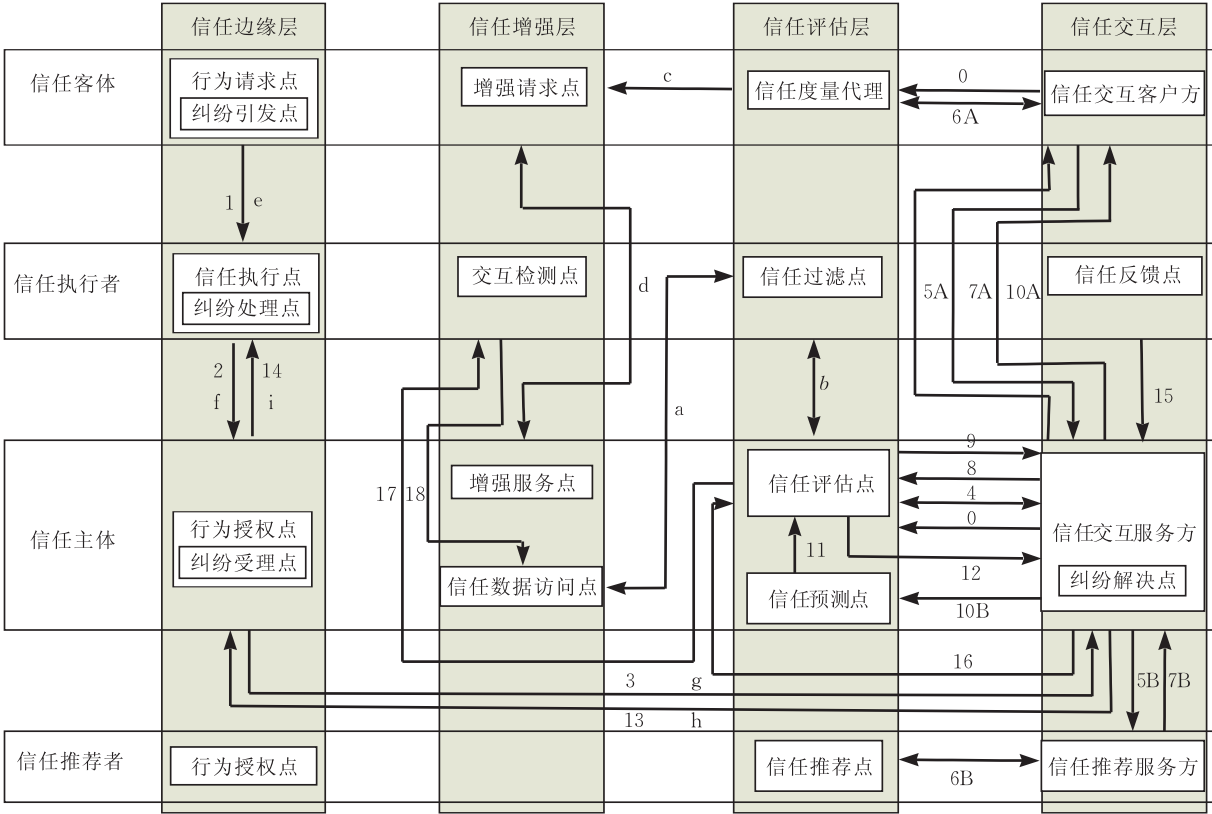


图 9 可信可控协议逻辑执行框架

信任控制部分(实现信任管理)

0. 在协议初始化阶段,TEC 发现、确认并加载 TMA, TES 检测 TEvP.
1. BRP 通告 TExP 信任客体的行为变化态势,TExP 也可通过监测信任客体处交互流量的办法感知到该通告.
2. 针对信任客体的行为变化态势,TExP 请求 BAP 实施信任评估.若 TExP 拥有控制此类行为变化态势的决策方案,则依此对信任客体实施相应的行为控制.
3. BAP 将该行为信任评估需求转发给 TES.
4. TEvP 检索(步 a 和 b)信任客体的行为信任记录,若存在,则转步 9.
- a 和 b. TEvP 通过 TFiP 和 TDAP 在网络中检索信任数据.
- 5A. TES 请求 TEC 提供信任证据信息用于实施信任评估.
- 5B. TES 请求 TRS 对信任客体的行为信任作出推荐.
- 6A. TEC 启动 TMA 来度量信任证据信息,并获取相应的结果.
- 6B. TRS 启动 TRP 检索信任记录,并返回相应的推荐信息.
- 7A. TEC 整合度量结果,并通过安全信道提交给 TES.
- 7B. TRS 将相关的推荐信息通过安全信道提交给 TES.
8. TES 初步分析所获取的信任评估信息后提交给 TEvP,同时等待信任评估的初步结果.

9. TEvP 基于预配置的评估规则对待评估信息进行信任评估,并将初步结果反馈给 TES.
- 10A. TES 将初步评估结果通告给 TEC,用于改善(步 c 和 d)信任客体信誉度.
- c 和 d. 依据 TEC 给予的信誉改善建议,ERP 与 ESP 进行协商并实施信誉改善.
- 10B. TES 将初步的信任评估结果提交给 TPP,等待最终决策.
11. TPP 依据所获得的初步评估结果,采用一定的策略(如贝叶斯网络、博弈分析等)进行实时动态的行为信任预测,并将预测结果提交给 TEvP.
12. TEvP 对初步评估结果和信任预测结果进行最终评估,并将结果反馈给 TES.
13. TES 依据最终评估结果进行决策,并将决策结果反馈给 BAP.
14. BAP 依据决策结果产生相应的控制指令,用于 TExP 对信任客体进行信任控制.
15. TFeP 对协议交互过程进行监测,并将所取得的信息通过安全信道提交给 TES.
16. TES 对监测信息进行处理,并以原始反馈信任流的形式提交给 TEvP 进行决策分析.
- 17 和 18. TEvP 将决策结果以历史信任反馈流的形式提交给 EDP,EDP 对信任流进行信任过滤,将最终信任数据通过 TDAP 在网络系统中存储,作为未来信任决策的依据.

纠纷处理部分(实现不可否认服务)

- e. 可信可控协议执行完成后,信任客体可能会对协议执行过程或结果有争议.此时,信任客体需要将纠纷处理请求连同其在协议执行期间收集到有关协议交互的防抵赖证据,通过 DTP 提交给 DDP 进行解决.
- f. 对所提交的纠纷处理请求,纠纷处理点 DDP 首先在本地策略库中寻找纠纷解决方案,并进行纠纷处理;若找不到,则需要通过 DDP 请求 DAP 受理该纠纷.
- g. DAP 对纠纷受理请求进行初步分析,主要是判断纠纷受理请求中所包含的防抵赖证据与协议轮的关联程度,若无关则不予受理,否则需要将受理结果以纠纷解决请求的形式提交给 DRP.
- h. DRP 充当纠纷解决过程中仲裁者角色,依据一定的原则对纠纷进行仲裁,并将仲裁结果反馈给 DAP.
- i. DAP 依据仲裁结果产生相应的纠纷处理指令,赋予 DDP 对纠纷进行实际处理.

图 10 给出了可信可控协议模型、控制方法与协议逻辑执行框架之间的关联:从控制过程角度给出的协议模型(图 3)体现在可信可控协议控制方法(图 7)中,从信任管理角度给出的协议模型(图 4)体现在可信可控协议逻辑执行框架(图 9)中,控制方法与执行过程的融合体现在感知器与信任边缘层、观测器与信任增强层、决策器与信任评估层、执行器与信任交互层的对应中,同时这种融合也保证了两个角度下协议模型的等价性.

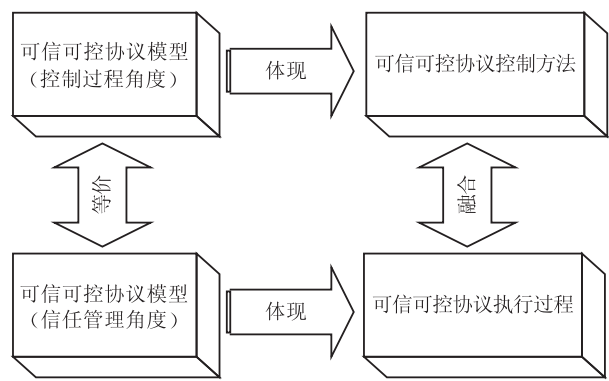


图 10 协议模型、控制方法与执行过程的关联

7 结束语

针对现有网络面临的安全与管理两大挑战,本文在不破坏现有网络体系结构的基础上,通过增加一个可信可控的 4 层逻辑结构创造性地提出一种可信可控的网络体系结构,以系统的、开放的、跨层的灵活方式解决网络的可信与可控问题,并继而给出了基于新体系结构的网络控制方法、可信可控协议

模型、协议控制方法和协议实施方案,以确保网络在满足方便管理的同时具备安全性.

虽然新的可信可控体系架构中数据流与控制流都通过跨层的可信接口层实现传输,占用了相同的信道,但两者在逻辑上实现了分离;该体系将一切基于时间序列的网络状态参数、用户行为参数、服务运行情况都以抽象层面的逻辑流形式来描述,实现了资源流和服务流在描述上的一致性,为描述的可观性提供了基础;基于该体系的新的控制方法,使得整个网络系统能以闭环自反馈形式运行,确保网络系统可以自诊断、自恢复地回归稳定态.本体系结构与现有技术相比,具有以下优点:

- (1) 融合了可信性与可控性,可满足多种网络运行目标,及时准确地建立网络连接视图,便于实施高效的网络控制,是对 4D 网络控制体系各层面功能的细化与补充.
  - (2) 建立了基于可信可观视图的一致性原则,且可信接口以跨层共享的模式打破了传统的协议分层模型,建立了协议的跨层设计,提供了以逻辑流为统一规范的资源流、信任流、控制流标准描述,可解决目前 4D 控制体系中网络管理逻辑集中化问题.
  - (3) 将传统的基于下一代网络的安全性研究推进到可信研究,并和网络管理机制结合,强调对用户行为的可信性及可控性测量与评估,改变传统网络中单一的防御、单一的信息安全补丁,为有效解决网络安全问题提供了新思路.
- 在完善可信可控网络体系的基础上,下一步工作集中在网络可信控制模型、控制机制与算法研究以及其它若干关键问题的研究,包括基于信任决策的系统预警、协同与资源控制机制,控制信息的语义描述、建模及处理机制,网络行为 and 用户行为的识别与监测机制,协议可信可控性验证;同时着手构建可信可控网络试验床,并进行相关的实际论证.

参 考 文 献

[1] Lin Chuang, Lei Lei. Research on next generation Internet architecture. Chinese Journal of Computers, 2007, 30(5): 694-711(in Chinese)  
(林闯,雷蕾. 下一代互联网体系结构研究. 计算机学报, 2007, 30(5): 694-711)

[2] Bavier A C, Feamster N, Huang M, Peterson L L, Rexford J. In VINI veritas: Realistic and controlled network experimentation//Proceedings of the ACM SIGCOMM'06. Pisa, Italy, 2006: 3-14



- [3] Clark D, Braden R, Falk A et al. FARA: Reorganizing the addressing architecture//Proceedings of the ACM SIGCOMM'03. Karlsruhe, Germany, 2003, 33(4): 313-321
- [4] Clark D, Wroclawski J, Sollins K R, Braden R. Tussle in cyberspace: Defining tomorrow's Internet//ACM SIGCOMM'02: Proceedings of the 2002 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications. Pittsburgh, PA, USA, 2002: 347-356
- [5] Greenberg A, Hjalmtysson G, Maltz D A et al. A clean slate 4D approach to network control and management. ACM SIGCOMM Computer Communication Review, 2005, 35(5): 41-54
- [6] Ballani H, Francis P. CONMan: Taking the complexity out of network management//Proceedings of the ACM SIGCOMM'06. Pisa, Italy, 2006: 41-46
- [7] Greenberg A, Hjalmtysson G, Maltz D A et al. Refactoring network control and management: A case for the 4D architecture. CS CMU: Technical Report CMU-CS-05-117, 2005
- [8] Caesar M, Caldwell D F, Feamster N et al. Design and implementation of a routing control platform//Proceedings of the NSDI'05. Boston, MA, USA, 2005: 15-28
- [9] Maltz D, Xie G, Zhan J et al. Routing design in operational networks: A look from the inside//Proceedings of the ACM SIGCOMM'04. Portland, Oregon, USA, 2004: 27-40
- [10] Xie G, Zhan J, Maltz D et al. On static reachability analysis of IP networks//Proceedings of the IEEE Infocom'05. Miami, Florida, USA, 2005: 2170-2183
- [11] Gu G, Luo J. Some issues on computer networks: Architecture and key technologies. Journal of Computer Science and Technology, 2006, 21(5): 708-722
- [12] Wu Jian-Ping, Bi Jun. The trustworthy next-generation Internet and its development. ZTE Communications, 2008, 14(1): 8-12(in Chinese)  
(吴建平, 毕军. 可信任的下一代互联网及其发展. 中兴通讯技术, 2008, 14(1): 8-12)
- [13] Zhang Hong-Ke, Su Wei. Fundamental research on the architecture of network — Universal network and pervasive services. Acta Electronica Sinica, 2007, 35(4): 593-598(in Chinese)  
(张宏科, 苏伟. 新网络体系基础研究——一体化网络与普适服务. 电子学报, 2007, 35(4): 593-598)
- [14] Meng Luo-Ming. Network management: Problems, progress and prospect. Journal of Beijing University of Posts and Telecommunications, 2003, 26(2): 1-8(in Chinese)  
(孟洛明. 网络管理研究中的问题、现状和若干研究方向. 北京邮电大学学报, 2003, 26(2): 1-8)
- [15] Lu Yu. Conception of Network Cybernetics. Beijing: National Defence Industry Press, 2005(in Chinese)  
(卢昱. 网络控制论概论. 北京: 国防工业出版社, 2005)
- [16] Peng X, Lin C. Architecture of trustworthy networks//Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing. Indianapolis, Indiana, 2006: 269-276
- [17] Srivatsa M, Xiong L, Liu L. TrustGuard: Countering vulnerabilities in reputation management for decentralized overlay networks//Proceedings of the 14th International Conference on World Wide Web. Chiba, Japan, 2005: 422-431
- [18] Sun Y, Han Z, Liu K J R. Defense of trust management vulnerabilities in distributed networks. IEEE Communications Magazine, 2008, 46(2): 112-119
- [19] Li J, Li R, Kato J. Future trust management framework for mobile ad hoc networks. IEEE Communications Magazine, 2008, 46(4): 108-114
- [20] ISO/IEC DIS 13888-1: Information technology-Security techniques-Non-repudiation-Part 1: General. ISO/IEC JTC1/SC27 N1503, October 1996
- [21] ISO/IEC DIS 13888-3: Information technology-Security techniques-Non-repudiation-Part 3: Using asymmetric techniques. ISO/IEC JTC1/SC27 N1507, October 1996
- [22] ISO/IEC DIS 13888-2: Information technology-Security techniques-Non-repudiation-Part 2: Mechanisms using symmetric techniques, ISO/IEC JTC1/SC27 N1679, April 1997
- [23] Ranganathan K. Trustworthy pervasive computing: The hard security problems//Proceedings of the 2nd Annual Conference on Pervasive Computing and Communications Workshops. Orlando, FL, USA, 2004: 117-121
- [24] Han Zhi-Geng, Luo Jun-Zhou, Wang Liang-Min. Extended-CSP based analysis of non-repudiation protocols. Journal on Communications, 2008, 29(10): 8-18(in Chinese)  
(韩志耕, 罗军舟, 王良民. 不可否认协议分析的增广 CSP 方法. 通信学报, 2008, 29(10): 8-18)



**LUO Jun-Zhou**, born in 1960, Ph.D., professor, Ph.D. supervisor. His research interests include next generation network architecture, protocol engineering, network security and management and grid computing.

**HAN Zhi-Geng**, born in 1976, Ph.D. candidate. His research interests include network security and cryptographic protocols.

**WANG Liang-Min**, born in 1977, Ph.D.. His research interests include cryptology and network security.

Background

This work is supported by the National Natural Science Foundation of China under grants No. 90604004 and 60773103, and the China Specialized Research Fund for the Doctoral Program of Higher Education under grant No. 200802860031, and the Jiangsu Provincial Natural Science Foundation of China under grants No. BK2007708 and BK2008030, and Jiangsu Provincial Key Laboratory of Network and Information Security under grant No. BM2003201, and the Key Laboratory of Computer Network and Information Integration (Southeast University), Ministry of Education under grant No. 93K-9.

Today’s Internet being one of the most important infrastructures in information society was designed based on the network architecture developed in the 1970s. However, with the repaid development of network technologies and applica-

tions, Internet is growing in size and complexity, some pre-suppositions and modes are changing, and new requirements are produced. Traditional network theories, especially the network security and management theories, are not good enough to support the network’s development, the network architecture is confronting some serious challenges on security and management, it is the time to rethink the network architecture for supporting trustworthiness and controllability.

With this issues in mind, the framework of a trustworthy and controllability network architecture is presented in this paper, including three essential properties, such as observability, controllability and reachable. Also the network control method, protocol model, protocol control method, protocol function and protocol implementing scheme are given out.