半 Markov 可信工业控制以太网研究 *

周森鑫[1,2], 韩江洪[1], 唐 昊[1]
(1. 合肥工业大学 计算机与信息学院, 合肥 230009; 2. 安徽财经大学 信息工程学院, 安徽 蚌埠 233041)

摘 要: 以可信计算和可信网络理论为基础,针对工业控制网络的特点构建可信工业控制网络理论架构。重点研究工业控制网络的安全性、可生存性和可控性等重要属性。以半马尔可夫网络流量模型为基础,建立半马尔可夫可信工业控制网络模型,定量分析其性能指标,得出可信度的量化公式。实验结果表明,该模型可行有效,能为可信工业控制网络设计和实现提供相关的理论指导。

关键词: 可信控制网络; 以太网; 半马尔可夫; 可生存性; 可控性
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2010)03-1047-05
doi:10.3969/j.issn.1001-3695.2010.03.067

Research of semi-Markov trusted industrial control Ethernet network

ZHOU Sen-xin[1,2], HAN Jiang-hong[1], TANG Hao[1]
(1. *School of Computer & Information, Hefei University of Technology, Hefei* 230009, *China*; 2. *School of Information Engineering, Anhui University of Finance & Economics, Bengbu Anhui* 233041, *China*)

Abstract: This paper set up trusted industrial control Ethernet network theory structure from its characteristics based on trusted computing and trusted network theories. Researched the performances of security, controllability and survivability importantly. Presented semi-Markov trusted industrial control Ethernet network model based on semi-Markov network traffic theory. Set up the trustworthy measure formula for industrial control Ethernet network. The results of simulation experiment show that the model can run availability and provide related theory instruction for trusted industrial control network.

Key words: trusted control network; Ethernet network; semi-Markov; controllability; survivability

随着互联网技术的发展与普及推广,Ethernet 技术也得到了迅速的发展,Ethernet 传输速率的提高和交换技术的发展,给解决 Ethernet 通信的非确定性问题带来了希望,并使 Ethernet 全面应用于工业控制领域成为可能。由于以太网具有应用广泛、价格低廉、通信速率高、软硬件产品丰富、应用支持技术成熟等优点,随着以太网通信速率的提高,全双工通信、交换技术的发展,为以太网通信确定性的解决提供了技术基础,从而为以太网直接应用于工业现场设备间通信提供了技术可能。目前它已经在工业企业综合自动化系统中的资源管理层、执行制造层得到了广泛应用,并呈现向下延伸直接应用于工业控制现场的趋势。从目前国际、国内工业以太网技术的发展来看,工业以太网在制造执行层已得到广泛应用,并成为事实上的标准。未来工业以太网将在工业企业综合自动化系统中的现场设备之间的互连和信息集成中发挥越来越重要的作用。据美国权威调查机构 ARC(Automation Research Company)报告指出,今后 Ethernet 不仅继续垄断商业计算机网络通信和工业控制系统的上层网络通信市场,也必将领导未来现场总线的发展,Ethernet 和 TCP/IP 将成为器件总线和现场总线的基础协议。我国也制定了发展高速以太网技术的战略,其目标是:攻克应用于工业控制现场的高速以太网的关键技术。其中包括解决以太网通信的实时性、可互操作性、可靠性、抗干扰性和本质安全等问题,同时研究开发相关高速以太网技术的现场设备、网络化控制系统和系统软件[1]。

虽然脱胎于 Intranet、Internet 等类型的信息网络,但是工业以太网是面向生产过程,对实时性、可靠性、安全性和数据完整性有很高的要求。既有与信息网络相同的特点和安全要求,也有自己不同于信息网络的显著特点和安全要求[2]。随着网络技术和应用的飞速发展,工业控制网络日益呈现出复杂、异构等特点,当前的网络体系已经暴露出严重的不足,工业控制网络正面临着严峻的安全和服务质量(QoS)保证等重大挑战,保障工业控制网络的可信成为其进一步发展的迫切需求。本文以可信计算和可信网络理论为基础,针对工业控制网络的特点构建可信工业控制网络理论架构。兼顾控制和网络的综合协同研究策略,重点研究工业控制网络的安全性、可生存性和可控性等重要属性。以半马尔可夫网络流量模型为基础,建立半马尔可夫可信工业控制网络模型,定量分析其性能指标,得出工业控制网络可信度的量化公式。

1 可信工业控制网络

1.1 可信网络研究分析

尽管人们提出可信系统的概念已经有一段历史,但国际上对可信网络的探索刚刚开始,基本概念和科学问题的认识还不深入。目前可信网络研究重点集中在下一代互联网的体系结

收稿日期: 2009-07-11; **修回日期**: 2009-09-07 **基金项目**: 国家自然科学基金资助项目(60404009);2009 年安徽省高校自然科学基金重大项目(ZD200905)

作者简介:周森鑫(1965-),男,副教授,硕导,博士研究生,主要研究方向为计算网络、数据挖掘(ahcdzsx@126.com);韩江洪(1956-),男,教授,博导,主要研究方向为智能控制技术、分布式系统;唐昊(1972-),男,教授,博士,主要研究方向为离散事件动态系统、神经元动态规划.

构方面,具体的研究目标为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[3]。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,并将信任关系转换为信任链,最终形成一个信任网络空间。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(CyberTrust)项目,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。在网络控制体系及关键问题方面,比较有影响力的是 CMU 牵头提出的网络控制与管理的 4D 结构和 GENI 计划支持的研究。4D 结构对现有网络体系进行了改进,在此基础上进一步提出了 4D 网络控制架构,将网络控制的四个环节映射成四个层面,即决策层、发现层、数据层和分发层。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。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[4]。

我国在网络可信性和可控性方面有着多年的研究。清华大学、东南大学等国内知名院校在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。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方面,清华大学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。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三个层次特性。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[3]。

1.2 可信工业控制网络

通过对可信网络的研究笔者发现,将可信网络理论应用于工业控制网络方面较为少见。根据现有的相关可信网络研究成果分析相对于互联网,工业控制网络的约束条件和特点更适合可信网络理论的应用和实现。首先工业控制网络的硬件和拓扑结构相对固定,从而使得信任空间容易建立和扩展;其次工业控制网络中的数据信息具有一定的规律性,便于控制实现可靠传输;同时工业控制网络对可信要求更为迫切,更具有实际应用价值,为此借鉴相关可信计算和可信网络理论提出可信工业控制网络的概念和相关的理论架构。

可信工业控制网络是指突破面向非连接 IP 网络“尽力而为”的业务模式,为占统治地位的实时控制信息交互业务以及各种异构接入网络应用提供良好的 QoS 保证的工业控制网络,即在不确定的 IP 网络基础上达到确定服务目标的控制网络。可信工业控制网络主要包括三个基本属性,即安全性、可生存性和可控性。本文以工业控制以太网为案例分别阐述其三个基本属性,建立半 Markov 网络流量可信工业控制以太网模型定量分析其性能指标,并通过实验仿真出一个可行的可信控制网络原型,从而为可信工业控制网络设计提供坚实的理论指导[5,6]。

1)安全性 针对工业控制网络,笔者认为安全性就是保证网络信息准确实时到达目的地,因而数据的真实性和实时性是安全性的核心问题。因此它具有显著特点和安全要求:工业控制以太网是一个网络控制系统,实时性要求高,网络传输要有确定性;整个企业网络按功能可分为处于管理层的通用以太网和处于监控层的工业以太网以及现场设备层(如现场总线)。管理层的通用以太网可以与控制层的工业以太网交换数据,上下网段采用相同协议自由通信;工业以太网中周期与非周期信息同时存在,各自有不同的要求。周期信息的传输通常具有顺序性要求,而非周期信息有优先级要求,如报警信息是需要立即响应的;工业以太网要为紧要任务提供性能保证服务,同时也要为非紧要任务提供尽力服务,所以工业以太网同时具有实时协议,也具有非实时协议。基于以上特点有以下安全要求:工业以太网应保证实时性不会被破坏,在商业应用中,对实时性的要求基本不涉及安全,而过程控制对实时性的要求是硬性的,常常涉及生产设备和人员安全;工业以太网的数据传输中要防止数据被窃取;必须保证经过授权的合法性和可审查性[7~12]。

2)可生存性 其关键特征是在遭受攻击、故障或意外事故时系统依然能够完成任务,并能在一定的时间内修复被损坏的服务的能力。系统在完成基本服务的同时仍然保持其基本属性,如数据完整性、机密性和可用性等。造成网络服务失效的因素很多,可能是系统运行过程中出现的软硬件故障,也可能是网络攻击或破坏等用户行为,甚至是一些自然因素。因此必须在理论上深入剖析独立于具体因素的可生存性的本质特征。容错、容侵和面向恢复的计算是几种典型的提高网络服务可生存性的方式。容错主要针对网络系统内部的故障,采用故障检测、故障允许、故障纠正等技术,减少系统对外界用户表现出来的错误的状态变迁。容侵则主要对抗用户的破坏和攻击行为,保障向合法用户提供服务的连续性,当然在性能上允许一定的衰减。容错和容侵主要是避免服务失效不同,面向恢复的计算则是解决如何在服务失效后能够快速恢复。可生存性主要解决网络故障的检测定位、网络系统的容错容侵、故障的纠正以及工业控制网络系统因采样和网络传输而影响控制性能等主要问题[8,9,13]。

3)可控性 网络的可控性是可信工业控制网络在设计上的一个重要属性。工业控制网络发展至今,已成为一个庞大的非线性复杂系统,如协议体系庞杂,业务种类繁多,异质网络融合发展。现有的一些控制手段显得非常薄弱,产生了许多的隐患。边缘论和面向非连接的设计思想保障了网络的高效互通,逐跳存储转发的分组传送方式简单灵活,无须在中间节点维护过多的状态信息,核心网络的工作集中于路由转发。这些机制的优点是设计简单、可扩展性强,然而却造成了分组传输路径的不可控,网络中间节点对传输数据包的来源不验证、不审计。

如何解决网络的低可控性与安全可信需求之间的矛盾,建立内在的、关联的工业控制网络可控模型,在理论和技术上仍是当前学术界的一个难题[10~12,14]。

2　半 Markov 网络流量可信工业控制以太网模型

本文以层次结构建立内在的、关联的半 Markov 网络流量可信工业控制以太网模型。该模型如图 1 所示。

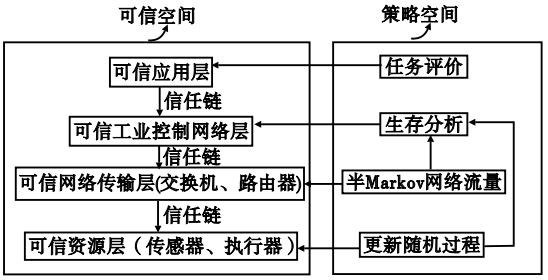

图1　半Markov网络流量可信工业控制以太网模型图

1)可信资源层　它是可信空间基层,主要是由传感器、执行器和通信线路等硬件资源组成。由于它们的可信本质特征主要是硬件故障行为,通过策略空间的更新随机过程定量描述:

$$S_o=0, S_n=\sum_{k=1}^{n}X_k, n\geqslant 1$$

其状态实现可控达到可信,并以此为基点建立可信空间。更新随机过程的定义如下:

定义 1　设$\{x_k, k\geqslant 1\}$是独立同分布,取值非负的随机变量,分布函数为 $F(x)$,且 $F(0)<1$ 令。

对$\forall t\geqslant 0$,记 $N(t)=\sup\{n: S_n\leqslant t\}$。

称$\{N(t), t\geqslant 0\}$为更新过程。$N(t)$表示在 t 时间内失效的硬件个数。对于 $N(t)$有如下定理成立:

定理 1　$P\left\{\lim\limits_{n\to\infty}\dfrac{N(t)}{t}=\dfrac{1}{\mu}\right\}=1$。

下面通过实例来说明上面定理具体的用法。假如一个传感器或执行器的寿命 X 为均匀分布在(30,60)内的随机变量,求长时间工作情况下它更换的速率为多少。若没有配件,获得该配件所需时间 Y 也是均匀分布的随机变量,均匀分布在(0,1),求更换该部件速率为多少。

$N(t)$表示在 t 时间内失效的硬件个数,长期工作的情况下,更新的速率为

$$\lim_{n\to\infty}\frac{N(t)}{t}=\frac{1}{\mu}$$

因 $\mu=E(x)=\int_{30}^{60}t\dfrac{1}{30}\mathrm{d}t=30\times\dfrac{1}{2}(60^2-30^2)=45$,故

$$\lim_{n\to\infty}\frac{N(t)}{t}=\frac{1}{45}=0.022\ 22$$

因此第一种情况下更换的速率为 0.022 22。

针对第二种情况:

$$\mu=E(X)+E(Y)=45+\int_0^1 t\mathrm{d}t=\frac{91}{2}$$

$$\lim_{n\to\infty}\frac{N(t)}{t}=\frac{1}{\mu}=\frac{2}{91}=0.021\ 98$$

因此第二种情况下更换的速率为 0.021 98。

2)可信网络传输层　硬件由交换机和路由器组成,完成数据传输和数据交换功能,是可信空间的核心层,也是最为复杂可控难度最大层。

工业控制信号有周期性实时数据、非周期性实时数据和软实时数据等。周期性实时数据包括从传感器定期地发往控制器和数据中心的信息,以及从控制中心定期传给执行机构的信息等。周期性实时数据和非周期性实时数据必须严格在规定时间内响应,否则将导致设备误操作,甚至整个控制系统崩溃。软实时数据的传输延时虽然不会造成灾难性的损失,但同样威胁系统的正常运行,必须避免。按照工业数据所需的实时要求分类:非周期性的网络控制信息或报警等约占工业数据量的 9.5%,最高优先级 7;非周期性的处理数据或事件约占工业数据量的 10%,短帧,优先级为 6;周期性的请求和响应处理数据约占工业数据量的 80%,短帧,优先级为 5;周期性的文件传输信息约占工业数据量的 0.5 %,长帧,优先级为 4;其他非实时的一般数据传输优先级较低为 0 ~3[15]。

在网络传输层中不可避免地存在网络诱导延时,主要包括网络等待延迟、数据在网络中的传输延迟和控制器节点的计算延迟。其大小主要与网络拓扑结构、网络负载状况、传输速率、数据包大小等有关。网络诱导延时可以是定常或时变的、确定或随机的、有界或无界的,它的存在会降低系统的性能,甚至使系统失稳,同时也会出现数据包丢失的现象。尽管多数网络协议具备重发机制,但仅仅在有限的时间内可以重发,等到时间过期,数据包也就被丢弃。从系统信息的传输来看,数据包丢失相当于信息传输通道暂时被断开,使得系统的结构和参数发生较大的变化,闭环控制系统虽然对系统中结构和参数的变化具有一定的鲁棒性,但是以降低系统的性能为代价,严重的丢包现象将导致系统失稳。由于网络带宽和数据包容量的限制难以将所有数据放在一个包中传输,从而造成数据包的时序错乱,势必也会影响系统的性能和稳定性[16]。

延时、丢包和多包传输的错序,是网络传输层中的三个基本问题。如何针对这些问题给出合理的可信评价是模型必须解决的关键问题。中国科学院计算技术研究所信息网络研究室黄晓璐等人引入半马尔可夫模型描述网络流量特性,通过忙阈值和闲阈值的设定,将网络流量划分为四种状态,即忙、空闲、上升和下降。研究各状态下的网络流量特性及各状态间的相互转换关系。通过网络协议性能分析,在一定的假设条件下推出 IP 网络流量在处于忙状态时服从几何布朗运动,在空闲状态下服从正态分布,在上升或下降状态下服从指数分布。半马尔可夫模型可以看做是马尔可夫模型的推广。其中心思想是针对不具有马尔可夫性的流,根据其不同特征划分为不同的状态,将对整个系统的研究转换为对不同状态的研究及对各状态之间转换性质的研究。半马尔可夫模型与马尔可夫模型的主要不同在于其状态之间的转移概率不是常数,而与状态保持时间分布有关[5]。本文通过设定忙阈值,将对网络传输层的系统可信评价转换为忙状态的时间分布函数,从而可定量描述网络传输层的可信值[2,17]。

3)可信工业控制网络层　本层在下面两层可信的基础上综合两层给出可信评价,如传感器、执行器设备故障和网络传输之间的关联引起的可信变化等。另外不同设备对整个网络的制约也不同,因而必须综合考虑。本文通过统计软件 SAS 中的生存分析技术来考察本层的可信值。

生存分析是指控制网络运行一定时间获得一定的相关生存数据,然后对生存时间的潜在分布情况进行描述,以及对生存时间与网络传输层及网络资源层可信值之间的关系进行探讨。生存分析的主要内容包括描述生存过程、比较生存过程以

及分析影响生存时间因素等。其基本方法分为非参数法、参数法和半参数法。各类方法又各自包含多种具体的分析方法。非参数法常用的方法包括极限法和寿命法等;参数法中常用的方法有指数分布法、威布尔分布法、对数正态回归分析法等;半参数法主要有 Cox 模型分析法等。针对具体情况,笔者选用参数法中的对数正态回归分析法。具体实现选用 SAS 生存分析中的 LIFEREG 过程。

LIFEREG 过程针对生存数据拟合有关生存时间的参数模型,所建立的模型为包含伴随变量和一个随机误差项的线性模型。其中误差项可来自多种分布形态的总体,包括极值分布、正态分布、Logistic 分布、指数分布等。其形式如下:

$$y = x'\beta + \sigma\varepsilon$$

其中:y 为应变量值组成的向量,是生存时间的对数;x 为若干协变量或自变量组成的矩阵;β 为需要估计的未知回归参数向量;σ 为未知的尺度参数;ε 为来自已知分布的误差向量。LIFEREG 过程应用 Newton-Raphson 算法,通过最大似然估计计算模型参数的估计值,应用观测值矩阵的逆矩阵来估计参数的标准误差。当对应变量的对数拟合模型时,这些模型等同于加速失效时间模型。加速失效时间模型中协变量间在失效时间上的效应是相乘的关系,一般情况下模型具有形如 $\exp(x'\beta)$ 的标准方程。假设 T_0 是来自基础分布(全部自变量均为 0)的一个样本失效时间,加速失效时间模型具有如下定义:

定义 2　设协变量向量为 x,则失效时间为 $T = \exp(x'\beta)T_0$。

具体的分析实例可见文献[18]。

4)可信应用层　这主要是针对用户的具体应用,可信评价由用户根据具体应用进行 QoS 评价。

3　实验与仿真

3.1　实验与仿真环境

本文选用的是 Ixia 公司的 Chariot 测试软件。Chariot 是一个独特的测试工具,能够评估网络应用的性能和容量,对网络和设备进行压力测试,得到设备及网络在不同应用、不同参数下的吞吐量、时延、丢包、反应时间等性能参数。Chariot 作为压力、故障定位、评估设备及网络应用层性能的测试软件,是维护健康、快速、可靠网络和研发生产高性能网络设备所需的可靠工具。目前被世界众多的知名企业、运营商、制造商和评测实验室所使用,包括 AT&T、北京通信、Cisco、IBM、Intel、Lucent、Tolly、中国信息产业部计量中心等,该产品已经成为网络性能测试的权威工具。

Chariot 由两部分组成,即控制端 Console 和远端 Endpoint。两者均可安装在普通 PC 或服务器上,控制端安装在 Windows 操作系统上,Endpoint 支持各种主流的操作系统。通过内置的脚本,由控制端控制远端相互主动发包,对设备进行功能、压力和性能等测试,测试结果包括吞吐量、时延、抖动、丢包、错包等,它能够得到定量的数据,并提供详尽的测试报告,从而使得用户可以主动地把握设备的性能状况,及时地发现问题并采取措施。

Chariot 通过各种机制可以仿真任意的应用。首先通过内置的脚本,Chariot 发送不同的数据流,可以模拟现在常见的 125 种应用,而且这种数据流是双向的,真正与协议栈进行交互。它对各种应用的支持是基于在 Endpoint 之间发送的多种数据流。数据流的传送可基于多种协议,包括 TCP、UDP、RTP、SPX、IPX 和 SNA,目前也已经支持 IPv6。Chariot 还支持 Multicast、QoS 等多种先进技术,而且将一直保持同步。另外,在出现新的或特殊的应用时,通过工具套件 Application Scanner 能够生成可以供 Chariot 使用的脚本。它允许对脚本进行定制,改变数据流的各种参数,如起始的启动间隔、发送窗口、接收窗口的大小、发送文件的大小、发送的速率、发送的比特流类型、使用端口等。这些参数不但可以是一个由用户指定的典型数值,而且还能选用在最大、最小值之间符合平均分布、正态分布、泊松分布或指数分布的随机值,从而真正地仿真网络中各种特定的数据流,全面地测试网络或网络设备在复杂的网络环境下的性能。

Chariot 最多可支持 10 000 个远端的协同测试,而远端软件则可以任意按照需要安装,在测试时即可被唤醒。具体有以下几个方面的应用:设备选型、基准性能测试、压力测试、功能测试、网络调整、网络性能展示以及性能瓶颈定位及排除等。在网络出现故障时,使用 Chariot 进行故障定位,判断是网络的问题还是服务器的问题,如果是网络的问题,再利用该工具进行定位。

3.2　实验与仿真设计

在 Chariot 服务器端,利用可视化设计工具根据具体测试任务设计测试拓扑结构图(图 2)。本文用两台主机 IP(地址为 192.168.153.1 和 192.168.153.3)仿真传感器和执行器,交换机的地址为 192.168.153.2,选择软件内置的 Throughput.scr 脚本可测量网络传输层的吞吐量、时延、丢包、反应时间等性能参数。

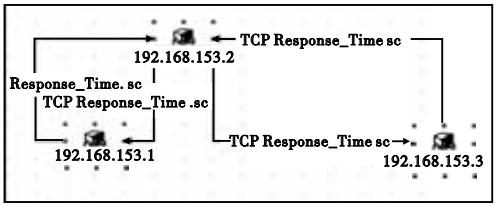

图2　实验仿真测试拓扑结构图

通过工具套件 Application Scanner 生成符合平均分布、正态分布、泊松分布或指数分布的随机值,测试脚本仿真网络中各种特定的数据流,通过设定忙阈值观察忙状态的时间分布,从而可定量计算网络传输层的可信值。本文在局域网络的多台主机中仿真构建实际锅炉控制系统,通过人为切断数据发送模拟传感器或执行器故障,利用 Chariot 软件进行故障检测和定位同时修改测试脚本中的数据包大小值,仿真工业控制网络的数据特征,通过复制测量项仿真实际控制网络中的多个数据传输通道,最后计算出网络资源层和网络传输层的可信值。在统计分析软件中,根据取得的相关历史数据计算出可信网络层的可信值。

4　结束语

本文以可信计算和可信网络理论为基础,针对工业控制网络的特点构建可信工业控制网络理论架构。兼顾控制和网络的综合协同研究策略,重点研究工业控制网络的安全性、可生存性和可控性等重要属性。以半马尔可夫网络流量模型为基础,建立半马尔可夫可信工业控制以太网模型定量,分析其各层性能指标,得出工业控制以太网可信度的量化公式。建立该

模型的实验仿真环境,并仿真构建实际锅炉工业控制以太网系统检验测试模型的可行性。仿真实验结果表明,该模型能有效定量反映工业控制以太网的可信性能。从掌握的资料分析目前国内有关工业控制网络可信评价的软件系统还是空白,笔者下一步研究的目标是以该模型为基础完善技术细节,通过 Chariot 和 SAS 软件相关 API 函数调用集成开发工业控制网络可信评价软件系统。

参考文献:

[1] 罗军舟,韩志耕,王良民. 一种可信可控的网络体系及协议结构[J]. 计算机学报,2009,32(3):391-404.

[2] 黄晓璐,闵应骅,吴起. 网络流量的半马尔可夫模型[J]. 计算机学报,2009,32(10):1592-1600.

[3] 李沁, 曾庆凯. 一种基于协议分析的可信信道评估方法[J]. 计算机学报,2009,32(8):1299-1366.

[4] 林闯,彭雪海. 一种可信可控的网络体系及协议结构[J]. 计算机学报,2005,28(5):751-758.

[5] 张怡,孙志刚. 面向可信网络研究的虚拟化技术[J]. 计算机学报,2009,32(3):417-423.

[6] Hu S,YAN Wei-yong. Stability of networked control systems: analysis of packet dropping [C]//Proc of International Conference on Control, Automation, Robotics and Vision. 2004: 304-309.

[7] ZHANG Ya , TIAN Yu-ping , CAI Jun. Stability analysis of networked control systems with packet loss [C]//Proc of the 6th World Congress on Control and Automation. 2006: 4556-4560.

[8] LIU Xiang-heng, GOLDSMITH A. Wireless communication tradeoffs in distributed control [C]// Proc of the 42nd IEEE Conference on Decision and Control. 2003: 688-694.

[9] ABADI M,TUTTLE M R . A semantics for a logic of authentication. [C]//Proc of the 10th Annual ACM Symposium on Principles of Distributed Computing . [S. L]:ACM Press,1991: 201-216.

[10] NILSSON J. Real-time control systems with delays [D]. Lund, Sweden: Department of Automatic Control, Lund Institute of Technology, 1998.

[11] LEE K C , LEE S. Remote controller design of networked control system using genetic algorithm[J]. IEEE International Symposium on Industrial Electronics, 2001, 1(3): 1845-1850.

[12] YANG Yue-quan, XU De, TAN Min. Hybrid and stochastic stabilization ana-lysis and H_∞ control for networked control systems [C]// Proc of IEEE Conference on Robotics, Automation and Mechatronics. 2004: 502-506.

[13] PARK H, KIM Y, KIM D, *et al*. A scheduling method for network-based control systems [J]. IEEE Trans on Control Systems Technology, 2002, 10(3): 318-330.

[14] CHAN H, OZGUNER U. Closed-loop control of systems over a communication network with queues [J]. International Journal of Control, 1995, 62(3): 493-510.

[15] ZHANG Wei . Stability analysis of networked control systems [D]. [S. l.]: Case Western Reserve University, 2001.

[16] RAY A, HALEVI Y. Integrated communication and control systems: Part II-design consideration [J]. ASME Journal of Dynamic Systems, Measurement and Control, 1988, 110(4): 374-381.

[17] NILSSON J , BERNHARDSSON B , WITTENMARK B. Stochastic analysis and control of real-time systems with random time delays [J]. Automatica, 1998, 34(1): 57-64.

[18] 薛富波,张文彤,田晓燕. SAS8.2 统计应用教程[M]. 北京:北京希望电子出版社,2004.

(上接第 1046 页)

从存储量来看,系统存储量包括公开信息大小和需要保密的秘密信息大小。对于秘密分发者来说,需要保密的信息仅为私钥 y;对于每个分享者来说,需要保密的信息同样仅为其私钥,其私钥 x_i 长度与所共享秘密 m 的长度相同,不会给系统造成过大的存储负担,因此,本文方案也是一个理想的方案。

从通信性能上来看,除了为分享者计算私钥时需要点对点的单播通信外,其余信息都可以通过广播形式进行传递。众所周知,广播是最有效、最节约能量的通信方式,而本文方案可以有效地利用广播通信方式, 因此具有较好的通信性能。

从实现过程上来看,与现有大多数方案相比,本文方案还有一个特点,就是分享者私钥(或秘密份额)的计算与秘密分发过程是分离的。本文以文献[1]的方案为代表与本文方案作一比较。文献[1]的方案包含三个过程,即系统参数建立、秘密分发和秘密重构过程。其中秘密分发过程融合了分享者私钥的计算。在本文方案中,因为分享者私钥计算可以预处理完成,而在分发秘密时,只需要一次广播即可;而文献[1]的方案事先无法预计算分享者私钥,只能在秘密分发过程中逐一安全发送,所以本文方案秘密分发效率更高。另外,在文献[1]的方案中,只要给分享者分发了私钥,就无法撤销所分享的秘密;而在本文方案中,秘密分发者还有权决定是否要分享某个秘密,因此,本文方案从秘密分发效率和安全性上更适合应用。

4　结束语

本文基于双线性变换构建了一个新的秘密分享方案。该方案将分享者私钥计算与秘密分发过程分离,可以重复利用秘密份额,是一个动态的秘密分享方案。本文方案是一个可证明安全的、有效的秘密分享方案,比现有方案更具安全性和有效性,更适合实际应用。

参考文献:

[1] SHAMIR A. How to share a secret [J]. Communications of the ACM, 1979, 24(11):612-613.

[2] BLAKLEY G. Safeguarding cryptographic key[C]//Proc of AFIPS 1979 National Computer Conference. 1979:313-317.

[3] JEFFERS J, ARAKALA A. Minutiae-based structures for a fuzzy vault[C]//Proc of IEEE Biometrics Symposium. 2006:760-769.

[4] 刘锋,何业锋,程学翰. 动态的(t,n)门限多秘密分享方案[J]. 计算机应用研究, 2008,25(1):240-241.

[5] ASMUTH C, BLOOM J. A modular approach to key safeguarding [J]. IEEE Trans on Information Theory, 1983, 29(2): 208-210.

[6] KARNIN E D, GREENE J W, HELLMAN M E. On sharing secret systems[J]. IEEE Trans on Information Theory, 1983, 29(1): 35-41.

[7] 庞辽军, 王育民. 一个基于几何性质的(t, n)多重秘密共享方案[J]. 西安交通大学学报, 2005, 39(4): 425-428.

[8] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[J]. SIAM Journal of Computation, 2003, 32(3): 586-615.