doi:10.3969/j.issn.1000-436x.2012.11.007

面向物联网的通用控制系统安全模型研究

杨金翠[1,2]，方滨兴[1,2]，翟立东[3]，张方娇[1,3]

（1. 北京邮电大学 计算机学院，北京 100876；
2．北京邮电大学 可信分布式计算与服务教育部重点实验室，北京 100876；3．中国科学院 信息工程研究所，北京 100093）

摘 要：物联网环境下，工业以太网和实时以太网的控制回路容易被利用进行恶意攻击，造成物理世界中重大的安全事故；通过分析物联网环境下控制系统的工作原理，提出物联网环境下的通用控制系统模型 IoTC，并以该模型为基础，讨论系统中可能面临的各种干扰因素；针对这些干扰因素，提出一种通用控制系统安全模型 S-IoTC，该模型通过在干扰处加入安全认证模块以保障系统安全性；最后就安全模型 S-IoTC 的组成部分、安全定理以及典型的实现过程进行了阐述。

关键词：物联网；控制系统；安全模型；干扰

中图分类号：TN91 **文献标识码：**A **文章编号：**1000-436X(2012)11-0049-08

Research towards IoT-oriented universal control system security model

YANG Jin-cui[1, 2], FANG Bin-xing[1, 2], ZHAI Li-dong[3], ZHANG Fang-jiao[1, 3]

(1.School of Computer Science and Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. Key Laboratory of Trustworthy Distributed Computing and Service, Ministry of Education, Beijing University of Posts and Telecommunications, Beijing 100876, China;3. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

Abstract: In Internet of things, the control loop of industrial Ethernet and real-time Ethernet is easily exploited by hackers for malicious attacks, causing serious security incidents in the physical world; a universal control system model (IoTC) was put forward by analysing the working principle of the control system in IoT, on which some disturbing factors the system faces were discussed; for the disturbing factors in the system, one universal control system security model (S-IoTC) was given, adding security authentication module in responding disturbing factor to achieve secure system; the components, safety justice and typical realization process of S-IoTC were also described in detail at last.

Key words: Internet of things; control system; security model; interference

1 引言

物联网是当前在国际上备受关注的前沿热点研究领域，已经引起了学术界和工业界的高度重视，被认为是对 21 世纪产生巨大影响力的技术之一。目前，随着物联网技术的不断发展和成熟，人们逐渐开始将物联网与控制系统进行有效结合，使它们充分发挥各自的优势，并广泛应用于工业制造、轨道交通、航空航天、军事、医疗卫生、灾害应急响应等领域。

收稿日期：2012-04-20；**修回日期：**2012-10-29
基金项目：国家高技术研究发展计划（“863”计划）基金资助项目（2011AA01A204）；国家自然科学基金资助项目（91118002）
Foundation Items: The National High Technology Research and Development Program of China (863 Program) (2011AA01A204); The National Natural Science Foundation of China (91118002)

物联网是一把双刃剑，它在给控制系统带来便利的同时，也带来了一些亟待解决的安全问题。长期以来，制造与生产企业的控制系统大都采用专用的、封闭的体系结构。然而，当控制系统与物联网相结合时，控制系统的体系结构也逐渐由封闭转向开放，工业以太网和实时以太网在控制回路中可能与远程互联，这就容易被黑客利用进行攻击。

2010年6月，世界上首个网络“超级武器”震网病毒(Stuxnet)[1~3]被检测出来，它是第一个专门攻击工业控制系统基础设施的病毒。震网病毒攻击了伊朗的浓缩铀工厂，这种病毒由被感染的U盘带入内部网络，传播到安装了西门子WinCC系统的主机后，通过修改发送至PLC的命令改变离心机的旋转速度，让离心机快速转动然后骤然降速使离心机受损，震网病毒对伊朗的工业设施造成了严重的损害。

由此可以看出，当封闭的控制系统与外界互联时，存在很多的不安全因素，一旦这些不安全因素被利用，将造成物理世界中重大的安全事故。物联网就是典型的例子，当物联网技术应用到工业控制等重要领域时，带来的不仅是更为智能化的系统、更为高效的管理、更为便捷的控制，同时还有更为严峻的安全挑战。

传统的物联网安全研究只关心2个要素：安全保护和隐私保护，其中安全保护包括了传统安全问题考虑的一些属性，如完整性、可用性、机密性等，是为了保护控制系统不被攻击；隐私保护是为了保护用户信息不被攻击。当物联网在控制系统上做应用时，需要考虑物联网的控制安全问题，即被控系统的安全问题。

对系统进行建模与分析是保证系统安全的重要手段。本文就从被控系统的安全问题角度出发，借鉴Petri网的描述方法，给出一种面向物联网的通用控制系统安全模型。

2 相关研究

目前，对面向物联网的控制系统安全的研究还处于起步阶段，针对面向物联网的控制系统的攻击模型、作用范围和危害程度还没有严格规范的描述。本节主要介绍物联网的体系结构及物联网在控制系统中应用的相关研究。

物联网的体系结构，在业界大致被公认为有3个层次，底层是用来感知数据的感知层，第二层是数据传输的网络层，最上面则是内容应用层[4]。还有一种说法是把应用层拆分成处理层和应用层，也就是认为物联网的体系结构，包括感知层、传输层、处理层和应用层4个层次[5]。

孙利民等在文献[5]中介绍了物联网的特征，包括其底层感知信息的时空特性和局部实时交互性，以及从对物理世界的感知、感知信息的传输和处理、对物理空间的反馈控制的开放式循环过程。探讨了物联网承载和处理巨海量信息的方式和结构，以及物联网体系结构需要考虑的问题。丁超等在文献[6]中基于IoT/CPS安全需求和威胁模型，提出了一种层次化的安全体系结构，并针对隐私保护、跨网认证和安全控制等IoT/CPS的关键安全技术展开了讨论。

关于物联网在控制系统中的应用，T.Tommila[7]等人在回顾自动化技术的报告中提到，工业自动化迫切需要更加智能化的控制系统平台，而信息技术在这一过程中起着至关重要的作用。SAP的研究报告[8]分析了物联网在制造行业中的应用，表示物联网在网络化智能物品方面有很大的创新。B. H. Kim等人在文献[9]中将M2M应用在智能制造系统中，并讲述了制造系统中的关键部分——运动控制系统的发展趋势，指出未来的控制系统将应用无线现场总线和泛在传感器网络。

国内也在广泛开展物联网在各行业中的应用研究。彭瑜在文献[10]中讨论了物联网的3个应用方向，并强调了其在工业应用方面的重要性。王建强在文献[11]中提出了基于物联网的感知矿山建设的总体框架，并从系统整合、拓展延伸和系统升华3个阶段系统全面的阐述了感知矿山的建设实施步骤，对物联网技术在感知矿山建设中的应用进行了详细的说明。李楠等在文献[12]中结合钢铁连铸设备的特点及存在的问题，提出了面向钢铁连铸设备维护、维修和大修的工业物联网架构，并讨论了框架实现的关键技术。曾韬在文献[13]中介绍了物联网在数字油田中的核心应用——油井生产远程监控系统，给出了系统架构，并对系统的3个子系统，即油井生产数据远程采集传输系统、油井生产远程分析管理系统、油井生产远程控制系统进行了描述。龚钢军等在文献[14]中根据智能电网信息通信技术平台的业务特点和功能需求，提出了面向智能电网输电、变电、配电和用电四大环节的物联网分层体系结构，并将其与传统电力通信网进行了对比。

3　面向工业控制的物联网系统标准体系结构

通常情况下，物联网的体系结构包括感知层、网络层和应用层。面向工业控制的物联网体系结构则需要体现出控制功能，通过分析物联网在各行业的具体应用情况，给出了面向工业控制的物联网系统标准体系结构，包括物理层、网络层和应用层，如图 1 所示，为了更好地体现物理世界、信息空间及人的感知互动关系，图中标出了感知事件流、控制信息流的流程。下面就对此图给出详细说明。

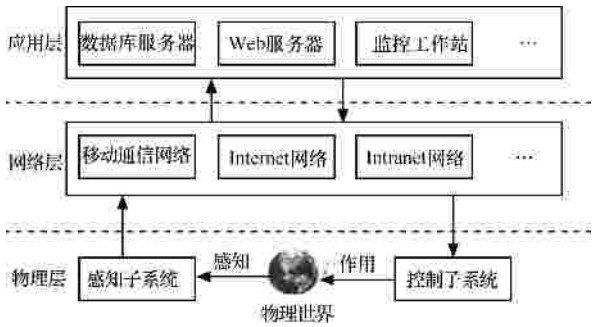

图 1　面向工业控制的物联网系统标准体系结构

1) 物理层

物理层由感知子系统和控制子系统构成，主要负责工业现场数据的感知，并根据系统指令对现场设备进行控制。感知对象包括工业对象、自然环境对象和智能安防等其他多种对象。

① 工业对象

根据物联网具体应用的背景，工业对象可包含多种对象。如物联网应用在煤矿中时感知工业对象包括井底瓦斯含量、矿井通风情况、矿井的矿压情况、有毒气体的检测情况以及井下人员的定位情况等。

② 自然环境对象

自然环境对象则涵盖温度、湿度、热量等环境因子。

③ 其他对象

其他对象包含各种负责安防监控的传感器、摄像头等短距离的通信设备。

2) 网络层

网络层完成工业物联网物理层与应用层之间的信息通信功能。网络层的通信网络可以是移动通信网络、Internet 网络、Intranet 网络等。

3) 应用层

应用层主要由各种应用服务器组成，完成对底层感知数据的汇聚、分析和存储。在通过传感手段获得的大量数据的基础上提供更加细粒度的管理和控制。

4　物联网环境下的通用控制系统模型 IoTC

物联网环境下控制系统的一个显著特征就是具有决策和控制功能，能够通过对物理世界的感知，对感知信息传输和处理，对事件进行判断和决策，再回到控制执行器进行执行动作，最终影响物理实体状态，形成从物理世界到信息空间再到物理世界的循环过程[5]。

总结以上可知，物联网控制系统的基本工作原理可以概括为：采集源点实现对被控对象或其他感知对象的感知识别，采集源点感知的信息经过传输通道到达决策点，决策点经过计算处理形成控制命令，控制命令经过控制通道下发给被控对象，实现对被控对象的控制。

现在用 S 表示采集源点，S_i（i=1,2,⋯,n）表示具体的数据来源，分为内部来源（如 S_1,S_2,⋯,S_k）和外部来源（如 S_{k+1},⋯,S_n），C_t 表示传输通道，D_p 表示决策点，C_m 表示控制通道，O 表示被控对象，t、t_i（i=1,2,⋯,n）表示瞬时变迁，得到物联网环境下控制系统的简单 Petri 网模型，如图 2 所示。

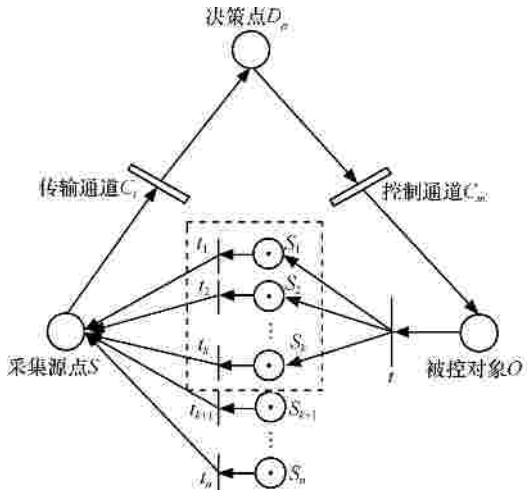

图 2　物联网环境下控制系统简单模型

图 2 中决策点处理过程较为复杂，可以将决策点的功能进一步细化，分为管理节点、控制算法和控制源点。管理节点：对控制策略进行管理；控制算法：进行控制计算；控制源点：下发控制命令。

现在用 C_p 表示管理节点，A 表示控制算法，C_s 表示控制源点，可以把图 2 进行扩展，得到不考

虑干扰因素的物联网环境下的控制系统 Petri 网模型，如图 3 所示。

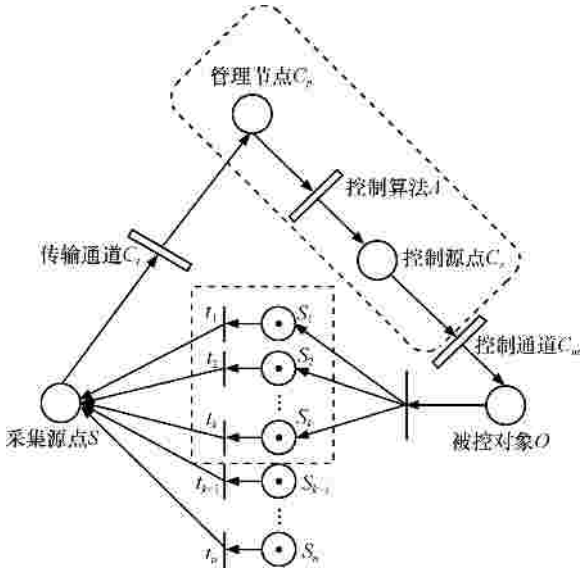

图 3 物联网环境下无干扰的控制系统模型

实际上，物联网环境下的控制系统，由于系统的复杂性及网络的开放性，可能会给物联网控制系统引进干扰因素。影响物联网控制安全的干扰因素可能来自以下几个方面。

1) 采集源点

物联网环境中的接入设备大多是处于无人值守状态下，这使得设备间的通信缺少了人为的监控和保护，物联网中的终端设备存在被人为破坏、非法盗用、被替换、被篡改等问题。另外，感知节点可能需要运行在极端恶劣的气候条件下，物理损坏、失效的概率也比较大。

2) 控制源点

物联网环境下的控制系统，控制点和被控制点存在分离的可能，由于控制源点在远程，导致控制源点可能被病毒感染、可能被恶意代码控制，甚至可能被替换，从而发送破坏性的控制命令。

3) 控制算法

物联网控制系统中的算法属于控制系统的核心，这部分的安全是极其重要的，实现了算法的安全才可能实现控制系统整体的安全。但是，由于系统的复杂性及网络的开放性，存在算法失效或算法被替换的风险。

4) 传输过程（传输通道、控制通道）

物联网是一个混合的网络，是由无线网络、有线网络以及包括各种设备的局域网共同组成的。在这样复杂的网络环境下，信息在传输过程中存在被截获、被篡改、被阻塞等安全隐患。

综上所述，物联网环境下的控制系统存在来源不确定性、传输安全（传输通道、控制通道）、算法安全等问题。

现在用 I_i（i=1,2,⋯,n）、I_a、I_b、I_c 表示干扰源，规定如下。

I_i（i=1,2,⋯,n）表示采集源点故障，包括采集源点失效或被攻击。

I_a 表示传输通道被攻击，导致采集信息在传输过程中被篡改或传输被阻塞。

I_b 表示算法故障，包括算法失效或算法被替换。

I_c 表示 a）控制源点失效、控制源点被攻击；b）控制通道被攻击，导致控制命令在传输过程中被篡改、传输被阻塞。

考虑以上干扰，得到物联网环境下通用控制系统 Petri 网模型 IoTC，如图 4 所示。

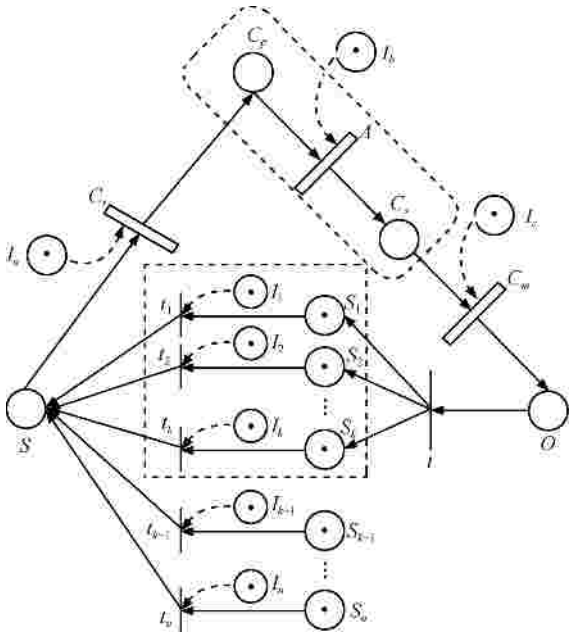

图 4 物联网环境下通用控制系统模型 IoTC

5 物联网环境下的通用控制系统安全模型 S-IoTC

针对物联网控制系统中可能存在的干扰因素，结合前面的物联网环境下通用控制系统模型 IoTC，提出了一个物联网环境下的通用控制系统安全模型 S-IoTC，如图 5 所示。

SM_i(i=1,2,⋯,n)表示在数据采集源 S_i(i=1,2,⋯,n)处增加的安全认证模块。

SM_a 表示在传输通道 Ct 处增加的安全认证模块。

SM_b 表示在控制算法 A 处增加的安全认证模块。

SM_c 表示在控制通道 C_m 处增加的安全认证模块。

下节将对此安全模型给出详细的说明。

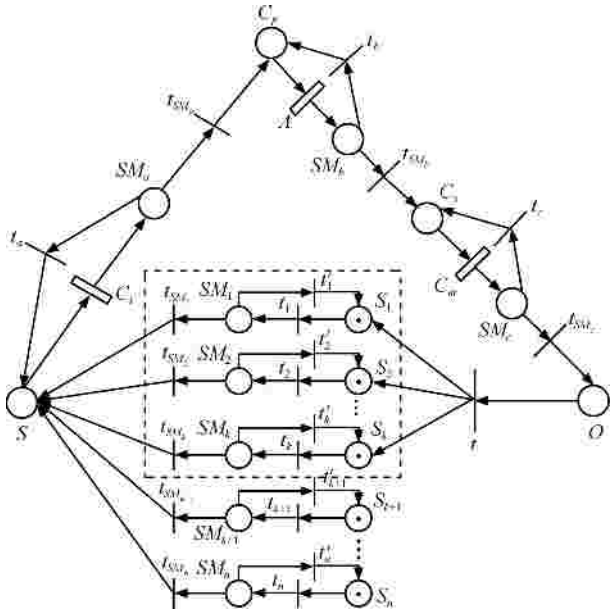

图 5　物联网环境下的通用控制系统安全模型 S-IoTC

5.1　S-IoTC 的组成部分

S-IoTC 需要刻画出物联网控制系统中各个要素，如采集源点、管理节点、控制源点、被控对象等之间的关系，由多个元素、相应关系和规则构成。

1) 元素

为了方便模型的形式化描述，将模型中涉及到的元素进行了数学形式的定义，定义物联网环境下的通用控制系统安全模型 S-IoTC 由四元组（P，T，F，M_0）组成，其中各个元素的含义如下，P：库所集合；T：变迁集合；F：弧集合；M_0：初始状态。

2) 相应关系—元素组成

定义 1　库所集合 P，包括 O、S_i、SM_i、S、SM_a、C_p、SM_b、C_s、SM_c，即 $P=\{O, S_i, SM_i, S, SM_a, C_p, SM_b, C_s, SM_c\}$，其中各个库所的含义如下。

O：被控对象。

S_i：具体的数据来源，分为内部来源（如 $S_1,S_2,\cdots,S_k$）和外部来源（如 $S_{k+1},\cdots,S_n$），其中 $i=1,2,\cdots,n$。

SM_i：安全认证模块，对数据采集源的安全性进行判断，其中 $i=1,2,\cdots,n$。

S：采集源点。

SM_a：安全认证模块，对传输通道的安全性进行判断。

C_p：管理节点，对控制策略进行管理。

SM_b：安全认证模块，对控制算法的安全性进行判断。

C_s：控制源点，下发控制命令。

SM_c：安全认证模块，对控制源点及控制通道的安全性进行判断。

定义 2　变迁集合 T，包括 t、t_i、t_i'、t_{SM_i}、C_t、t_a、t_{SM_a}、A、t_b、t_{SM_b}、C_m、t_c、t_{SM_c}，即 $T=\{t, t_i, t_i', t_{SM_i}, C_t, t_a, t_{SM_a}, A, t_b, t_{SM_b}, C_m, t_c, t_{SM_c}\}$，其中变迁 C_t 表示数据在传输通道传输过程、A 表示控制算法执行过程、C_m 表示数据在控制通道传输过程，它们具有时间特性，因此用矩形框表示；其他变迁均为瞬时变迁，用线段表示。变迁集合中各个变迁的含义如下。

t：采集点从被控对象采集数据。

t_i：采集信息汇聚到采集源点，其中 $i=1,2,\cdots,n$。

t_i'：数据未通过 SM_i 安全认证，需要重新采集，其中，$i=1,2,\cdots,n$。

t_{SM_i}：数据通过 SM_i 安全认证，正常流转，其中 $i=1,2,\cdots,n$。

C_t：传输通道，采集数据从采集源点 S 传输给管理节点 C_p。

t_a：数据未通过 SM_a 安全认证，需要重新传输。

t_{SM_a}：数据通过 SM_a 安全认证，正常流转。

A：控制算法，进行控制计算。

t_b：数据未通过 SM_b 安全认证，需要重新计算。

t_{SM_b}：数据通过 SM_b 安全认证，正常流转。

C_m：控制通道，控制命令从控制源点下发给被控对象。

t_c：数据未通过 SM_c 安全认证，需要重新传输。

t_{SM_c}：数据通过 SM_c 安全认证，正常流转。

定义 3　弧集合 $F=\{<O, t>, <t, S_i>, <S_i, t_i>, <t_i, SM_i>, <SM_i, t_i'>, <t_i', S_i>, <SM_i, t_{SM_i}>, <t_{SM_i}, S>, <S, C_t>, <C_t, SM_a>, <SM_a, t_a>, <t_a, S>, <SM_a, t_{SM_a}>, <t_{SM_a}, C_p>, <C_p, A>, <A, SM_b>, <SM_b, t_b>, <t_b, C_p>, <SM_b, t_{SM_b}>, <t_{SM_b}, C_s>, <C_s, C_m>, <C_m, SM_c>, <SM_c, t_c>, <t_c, C_s>, <SM_c, t_{SM_c}>, <t_{SM_c}, O>\}$。

定义 4　初始状态为 M_0，各个库所中元素的初

始化值为：$M_0(O)=0$, $M_0(S_i)=1$, $M_0(SM_i)=0$, $M_0(S)=0$, $M_0(SM_a)=0$,$M_0(C_p)=0$, $M_0(SM_b)=0$, $M_0(C_s)=0$, $M_0(SM_c)=0$。

3) 状态转换规则

状态转换规则主要是用来描述系统中状态的迁移情况。在 S-IoTC 中的状态转换主要包括以下几个规则。

规则 1 transition_disturb_collect_0 规则,用于表示数据采集过程中未受到任何干扰,即 $\neg I_1 \wedge \neg I_2 \wedge \neg I_3 \wedge \cdots \wedge \neg I_n$。数据经过安全认证模块 SM_i（i=1,2⋯,n）的检测，确认为安全数据，数据到达采集源点 S。

规则 2 transition_disturb_collect_1 规则，用于表示数据采集过程受到干扰源 I_i（i=1,2,⋯,n）中的 1 个或多个干扰，受干扰的数据未通过对应安全认证模块 SM_i 的检测，数据流被阻断，数据需要重新采集。

规则 3 transition_disturb_transmit_0 规则，用于表示数据传输过程 C_t 未受到干扰，即 I_a 未发生。要传输的数据经过安全认证模块 SM_a 的检测，确认为安全数据，数据到达管理节点 C_p。

规则 4 transition_disturb_transmit_1 规则，用于表示数据传输过程 C_t 受到干扰源 I_a 干扰,数据未通过安全认证模块 SM_a 的检测，数据流被阻断，数据需要重新从采集源点 S 传送。

规则 5 transition_disturb_algorithm_0 规则，用于表示控制算法 A 未受到干扰，即 I_b 未发生，数据经控制算法 A 处理后，经过安全认证模块 SM_b 的检测，确认为安全数据，数据流向控制源点 C_s。

规则 6 transition_disturb_algorithm_1 规则，用于表示控制算法 A 受到干扰源 I_b 干扰，数据未通过安全认证模块 SM_b 的检测，数据流被阻断，需要重新计算。

规则 7 transition_disturb_control_0 规则,用于表示控制源点 C_s 和控制通道 C_m 未受到干扰，即 I_c 未发生，控制命令经过安全认证模块 SM_c 的检测，确认为安全数据，控制命令下达至被控对象 O，实施控制。

规则 8 transition_disturb_control_1 规则，用于表示控制源点 C_s 或者控制通道 C_m 受到干扰源 I_c 干扰，数据未通过安全认证模块 SM_c 的检测，数据流被阻断，控制命令需要重新从控制源点 C_s 下达。

5.2 S-IoTC 的安全定理

定理 S-IoTC 是安全的。

S-IoTC 模型安全性即指从数据采集源点采集到的数据经过一系列的传输和处理，最后形成控制命令到达被控对象，整个过程都是安全的。

因为没有绝对的安全，规定物联网通用控制系统的安全阈值为 a，假设数据进行安全模块 SM_j（j=1,2,⋯,n,a,b,c）认证时，得到的安全概率为 $ß$，如果 $ß>a$，我们就认为数据是安全的，可以通过安全模块 SM_j（j=1,2,⋯,n,a,b,c）的认证。

1) 采集源点安全性

各采集点 S_i（i=1,2,⋯,n）采集的数据如果成功到达采集源点 S，必然是通过了安全模块 SM_i（i=1,2,⋯,n）的认证，这表明采集源点的安全概率高于安全阈值，可以认为采集源点是安全的。

2) 传输通道安全性

采集源点采集到的数据，如果经过传输通道 C_t 成功传送到管理节点 C_p，必然是通过了安全模块 SM_a 的认证，这表明传输过程的安全概率高于安全阈值，可以认为传输通道是安全的。

3) 算法安全性

如果系统信息经过控制算法 A 成功到达控制源点 C_s，必然是通过了安全模块 SM_b 的认证，这表明控制算法的安全概率高于安全阈值，可以认为控制算法是安全的。

4) 控制源点及控制通道安全性

如果控制命令从控制源点 C_s 经控制通道 C_m 成功下达到被控对象 O，必然是通过了安全模块 SM_c 的认证，这表明控制源点和控制通道的安全概率高于安全阈值，可以认为控制源点及控制通道是安全的。

由以上，即可证明 S-IoTC 模型是安全的。

5.3 S-IoTC 的实现过程

S-IoTC 模型的实现过程如图 6 所示，其基本实现过程由以下几个步骤组成。

Step1 从被控对象 O 或其他采集点采集数据。

Step2 采集的数据到达采集源点 S 前，要经过安全认证模块 SM_i（i=1,2,⋯,n）的认证，确认数据采集过程是否受到干扰源 I_i（i=1,2⋯,n）干扰。

Step3 没有通过 SM_i 安全认证的数据将被阻断，经过状态转换规则 2-transition_disturb_collect_1 转换，数据流转返回数据采集点，数据需重新采集；通过认证的数据，经过状态转换规则 1- transi-

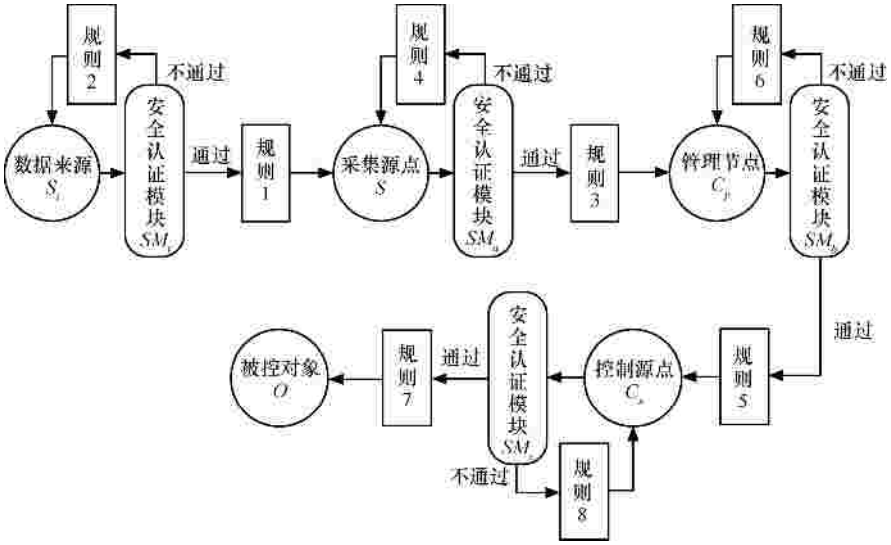

图 6　S-IoTC 实现过程

tion_disturb_collect_0 **转换，数据进行正常流转至采集源点** S**。**

Step4　数据由采集源点 S **传输到管理节点** C_p **时，数据要经过安全认证模块** SM_a **认证，确认数据传输过程是否受到干扰源** I_a **干扰。**

Step5　没有通过 SM_a **安全认证的数据将被阻断，经过状态转换规则** 4-transition_disturb_ transmit_1 **转换，数据流转返回采集源点** S**，数据需重新传输；通过认证的数据，经过状态转换规则** 3-transition_ disturb_ transmit _0 **转换，数据进行正常流转。**

Step6　数据从管理节点经过控制算法 A **到达控制源点前，要经过安全认证模块** SM_b **认证，确认控制算法是否受到干扰源** I_b **干扰。**

Step7　没有通过 SM_b **安全认证的数据将被阻断，经过状态转换规则** 6-transition_disturb_ algorithm_1 **转换，数据流返回，需要重新计算；通过认证的数据，经过状态转换规则** 5-transition_ disturb_algorithm_0 **转换，数据进行正常流转至控制源点** C_s**。**

Step8　控制源点 C_s **根据控制算法的处理结果下发控制命令到被控对象** O**，数据要经过安全认证模块** SM_c **认证，确认控制源点及控制通道是否受到干扰源** I_c **干扰。**

Step9　没有通过 SM_c **安全认证的数据将被阻断，经过状态转换规则** 8-transition_disturb_ control _1 **转换，数据流返回，控制命令需重新下发；通过认证的数据，经过状态转换规则** 7-transition_ disturb_control_0 **转换，控制命令下发至被控对象** O**。**

6　结束语

物联网是当前在国际上备受关注的前沿热点研究领域，并且已被逐渐应用到工业制造、轨道交通、航空航天等自动控制领域。物联网在给控制系统带来便利的同时，也带来了一些亟待解决的安全问题。对系统进行建模与分析是保证系统安全的重要手段。本文就从被控系统的安全问题角度出发，通过分析物联网环境下控制系统的工作原理及面临的干扰因素，提出了物联网环境下的通用控制系统模型 IoTC **及通用控制系统安全模型** S-IoTC**，并阐述了安全模型** S-IoTC **的组成部分、安全定理以及典型的实现过程。**

参考文献：

[1] FALLIERE N, MURCHU O L, CHIEN E. W32.Stuxnet Dossier[R].Symantec Security Response,2011.

[2] MATROSOV A, RODIONOV E, HARLEY D.Stuxnet Under the Microscope[R].ESET.

[3] LARIMER J.An inside look at Stuxnet[R].IBM.

[4] **江代有. 物联网体系结构、关键技术及面临问题**[J].**电子设计工程**, 2012,20(4):143-145.
JIANG D Y. Internet of things architecture,key technologies and issues facing[J]. Electronic Design Engineering, 2012, 20(4):143-145.

[5] **孙利民,沈杰,朱红松.从云计算到海计算：论物联网的体系结构**[J].**中兴通信技术**,2011,17(1):3-7.
SUN L M, SHEN J, ZHU H S. From cloud computing to sea computing: the architecture of the Internet of things[J]. ZTE Technology Journal,2011,17(1):3-7.

[6] 丁超, 杨立君, 吴蒙. IoT/CPS 的安全体系结构及关键技术[J]中兴通信技术, 2011,17(1):11-16.
DING C, YANG L J, WU M. Security architecture and key technologies for IoT/CPS[J]. ZTE Technology Journal, 2011, 17(1):11-16.

[7] TOMMILA T, VENTA O, KOSKINEN K. Next GenerationIndustrial Automation-Needs and Opportunities, AutomationTechnology Review[R]. 2001.34-41.

[8] LOGEAISG. Internet of Things in the Context of Manufacturing[R]. SAPResearch Report.

[9] KIM H B,YOO M,CHO K. Application of M2M technology to manufacturing systems[A]. Information and Communication Technology Convergence[C]. 2010. 519-520.

[10] 彭瑜.物联网技术的发展及其工业应用的方向[J].自动化仪表,2011,32(1):1-7.
PENG Y. Development of the Internet of things and its orientation in industrial applications[J]. Process Automation Instrumentation, 2011, 32(1):1-7.

[11] 王建强.物联网在感知矿山建设中的应用研究[J].中国安全生产科学技术,2012,8(5):178-183.
WANG J Q. Application of IOT in construction of sensor mine[J]. Journal of Safety Science and Technology, 2012, 8(5):178-183.

[12] 李楠, 刘敏, 严隽薇. 面向钢铁连铸设备维护维修的工业物联网框架[J]. 计算机集成制造系统,2011,17(2):413-418.
LI N, LIU M,YAN J W. Framework for industrial Internet of things oriented to steel continuous casting plant MRO[J]. Computer Integrated Manufacturing Systems, 2011, 17(2):413-418.

[13] 曾韬. 物联网在数字油田的应用[J] .电信科学,2010,26(4):25-32.
ZENG T. IoT's Application in the "Digital Oil Field" [J]. Telecommunications Science, 2010,26(4):25-32.

[14] 龚钢军, 孙毅, 蔡明明. 面向智能电网的物联网架构与应用方案研究[J]. 电力系统保护与控制,2011,39(20):52-58.
GONG G J, SUN Y, CAI M M. Research of network architecture and implementing scheme for the Internet of things towards the smart grid[J]. Power System Protection and Control, 2011,39(20):52-58.

作者简介：

杨金翠（1969-），女，山西侯马人，北京邮电大学博士生，主要研究方向为信息安全、物联网安全、软件工程等。

方滨兴（1960-），男，江西万年人，中国工程院院士，北京邮电大学校长、博士生导师，主要研究方向为网络安全、信息内容安全、并行处理、互联网技术等。

翟立东（1982-），男，山西祁县人，博士，中国科学院副研究员，主要研究方向为融合网络安全监测、网络攻防、数据挖掘、物联网控制安全等。

张方娇（1989-），女，山东新泰人，北京邮电大学硕士生，主要研究方向为物联网安全。

（上接第 48 页）

[2] ALMENAREZ F, MARIN A, CAMPO C, *et al.* TrustAC: trust-based access control for pervasive devices[A]. LNCS 450[C]. Berlin, Germany, 2005. 225-238.

[3] AHAMED S I, SHARMIN M. A trust-based secure service discovery (TSSD) model for pervasive computing[J]. Journal of Computer Communications, 2008,31(18):4281-4293.

[4] AHAMED S I, HAQUE M M. Design, analysis, and deployment of omnipresent formal trust model (FTM) with trust bootstrapping for pervasive environments[J]. Journal of Systems and Software, 2010, 83(2): 253-270.

[5] TAHERIAN M, JALILI R, ABOLHASSANI H, *et al.* PTO: a trust ontology for pervasive environments[A]. IEEE AINA-2008 International Conference[C]. Gino Wan, Okinawa, Japan, 2008.301-306.

[6] HE R, NIU J W, ZHANG G W. CBTM: a trust model with uncertainty quantification and reasoning for pervasive computing[A]. LNCS 3758[C]. Berlin, Germany, 2005. 541-552.

[7] MELAYE D, DEMAZEAU Y. Bayesian dynamic trust model[A]. LNCS 3690[C]. Berlin, Germany, 2005. 480-489.

[8] DUMA C, SHAHMEHRI N. Dynamic trust metrics for peer-to-peer system[A]. Proc of the 16th Int'l Workshop on Database and Expert Systems Applications (DEXA 2005)[C]. Washington, USA, 2005. 776-781.

[9] KAELBLING L P, LITTMAN M L, MOORE A W. Reinforcement learning: a survey[J]. Journal of Artificial Intelligence Research, 1996, 4:237-285.

作者简介：

王江涛（1977-），男，湖南郴州人，长沙大学讲师，主要研究方向为普适计算网络环境中的可信模型研究、上下文感知可信模型。

陈志刚（1964-），男，湖南益阳人，博士，中南大学教授、博士生导师，主要研究方向为网络计算与分布式处理。

邓晓衡（1974-），男，湖南衡阳人，博士，中南大学副教授，主要研究方向为流量管理、网络拥塞控制、网络优化、网格计算等。